Aadhaar Verification Implementation Guide

Overview:

This guide explains two methods for Aadhaar verification in a secure and automated manner-1) OCR-based document verification using Tesseract, and 2) API-based Aadhaar QR authentication via DigiLocker's API Setu.

---

1. OCR-Based Aadhaar Document Verification

Purpose:

Extract text fields (name, Aadhaar number, DOB) from uploaded Aadhaar images and validate them against user-entered data.

Tools Used:

- Tesseract OCR (via tesseract.js or Jimp + qrcode-reader in Node.js)
- Jimp for image processing
- Custom scoring logic to determine document authenticity

Implementation Steps:

1. Accept Aadhaar image upload via frontend.
2. On the backend:
- Use `Jimp` to read the image.
- Extract embedded QR code using `qrcode-reader` (if available).
- Fallback to Tesseract OCR if QR is not present or unreadable.

3. Parse the extracted text (e.g., using regex or XML parsing).

4. Compare extracted name and DOB to registered user details.

5. Score result (e.g., 0-10) based on confidence and text match.

6. Accept scores >= 5 automatically; send lower scores to admin.

Benefits:

- Fast and lightweight

- Fully local (privacy preserved)

- Easy fallback when QR is unreadable

Limitations:

- Accuracy depends on image quality

- No cryptographic signature verification

---

2. Aadhaar QR Verification via DigiLocker API Setu

Purpose:

Verify Aadhaar identity through government-issued APIs with higher security and official data validation.

Platform:

- DigiLocker API Setu (https://apisetu.gov.in)

- Issuer: UIDAI (Unique Identification Authority of India)

Process:

1. Registration:

- Sign up on DigiLocker's [Partner Portal](https://partner.digilocker.gov.in).

- Apply for API access under the UIDAI issuer category.

- Provide required documents and organization details.

- Await approval and access credentials.

2. Integration:

- Use the provided Client ID and Secret to authenticate.

- Obtain access tokens for secure API calls.

- Call the Aadhaar Document Pull API or QR Reader API.

- Receive verified XML/JSON containing Aadhaar fields.

- Parse the response and store verified data securely.

3. Security Measures:

- HTTPS mandatory for all API calls.

- Ensure request integrity and log verification requests.

- Follow UIDAI data handling protocols strictly.

Benefits:

- Data directly verified with UIDAI.

- QR signature verified (non-editable).

- High confidence and legally recognized.

Limitations:

- Requires formal onboarding process.

- API rate limits and compliance logging required.

Conclusion:

Combining both OCR-based and DigiLocker API-based verification ensures maximum coverage and flexibility. Start with OCR for basic validation and fallback. For verified government data, integrate with DigiLocker API Setu to gain access to tamper-proof, UIDAI-authenticated Aadhaar verification.