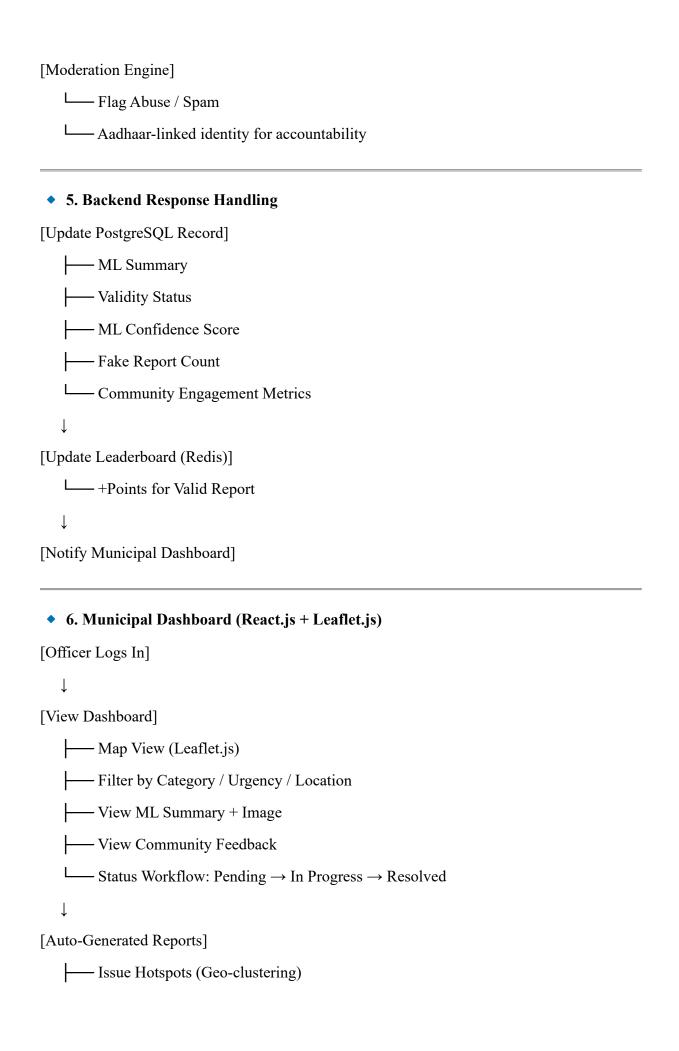
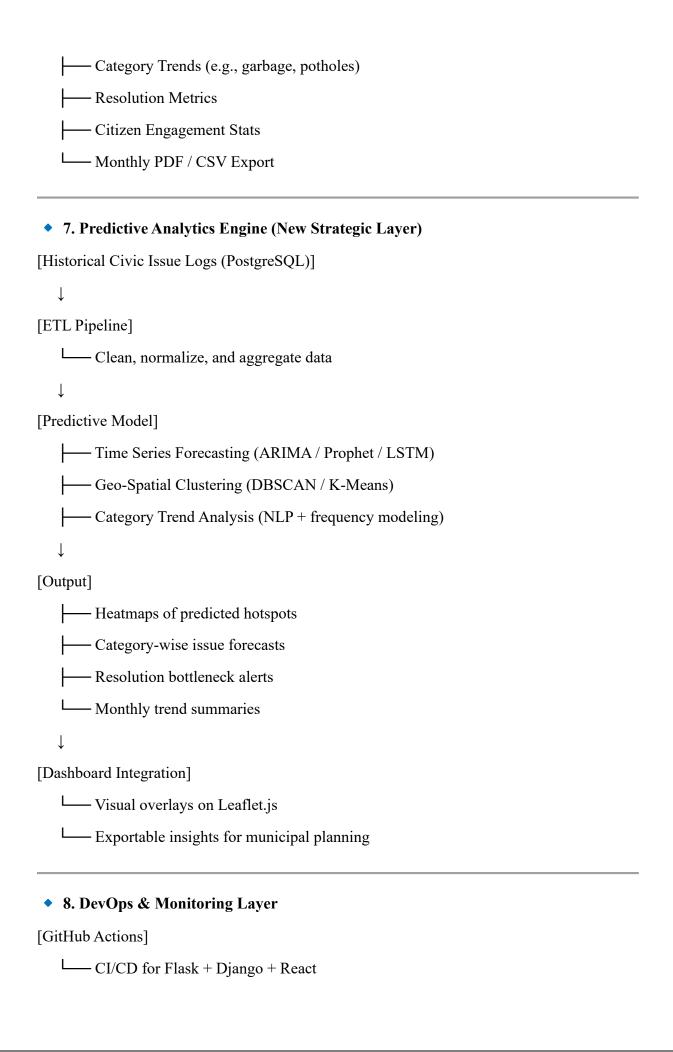
• 1. Citizen Interaction Layer (Mobile App – Java) [User Launches App] [Login / Aadhaar Authentication] [Submit Civic Issue] Capture Image Auto-fill Summary (via on-device ML) GPS Location Category Selection Language Selection (Multilingual UI) \downarrow [Local Storage (RoomDB) if Offline] \downarrow [Send to Backend via REST API] • 2. Backend Gateway (Django REST + JWT) [Receive Report] \downarrow [Verify JWT Token + Aadhaar Status] \downarrow [Store Metadata in PostgreSQL] — User ID Location — Timestamp Category Language Aadhaar Masked ID

```
[Upload Image to AWS S3]
   \downarrow
[Trigger ML Pipeline via Flask Microservice]
 • 3. ML Pipeline (Flask + TensorFlow + Transformers)
[Flask Endpoint: /validate-report]
   \downarrow
[Run Fake Report Detection]
   Image Analysis (CNN)
   Text Analysis (Transformer based architecture)
   Duplicate Check (pHash)
   \downarrow
[If Valid \rightarrow Proceed]
[If Fake \rightarrow Flag User]
   Increment Fake Count
   If Fake Count > 3 \rightarrow Restrict User + Notify Admin
[Run Image Captioning Model]
      — Generate Auto-Summary
   \downarrow
[Return Summary + Validity Flag to Backend]
 • 4. Community Layer
[Access Community Section]
   — View Local Issues
     — Comment / Discuss
   Upvote / Downvote Reports
   Multilingual Threads (Auto-translate via NLP)
```





[Prometheus + Grafana]
Monitor API Health, ML Latency, Dashboard Uptime
[AWS / GCP]
Host Services + Auto-Scale
[Docker + NGINX]
Containerization + Routing
• 9. Security & Governance Layer
[Aadhaar eKYC API]
L—OTP Verification
└── Masked ID Storage
[JWT Authentication]
Role-Based Access (Citizen / Officer / Admin)
[User Restriction Logic]
Flag + Lock after 3 fake reports
[Data Encryption]
L—AES for PII
HTTPS for All Traffic