

The Problem We're Solving

Citizens face several challenges when reporting civic issues:

- Low app adoption in some areas means no community to verify reports
- Fake or spam reports waste municipal resources
- GPS can be spoofed to submit false locations
- Duplicate reports create confusion and extra work
- Emergency issues need faster processing than normal reports
- Reports can be deleted or altered without accountability

Our Solution: Multi-Layered Verification

Instead of relying on just one verification method, StreetLight uses multiple layers that work together. Think of it like airport security with multiple checkpoints - if one checkpoint has an issue, others can still catch problems.

Key Features

- **No Single Point of Failure:** If community verification fails (no users nearby), AI and location checks can still approve genuine reports
- **Smart Scoring System:** Every report gets a confidence score (0-100) based on multiple signals
- **Fraud Detection:** Automatically catches GPS spoofing, duplicate reports, and coordinated fake submissions
- **Blockchain Accountability:** Verified reports are permanently recorded and cannot be deleted or altered
- **Human Oversight:** Municipal officers can review edge cases and override AI when needed

How the System Works

When a citizen submits a report, it goes through multiple verification layers. Here's the complete flow:

Step 1: User Submission

1. Citizen opens the mobile app
2. Takes a photo of the civic issue (pothole or garbage)
3. GPS automatically captures location
4. Submits the report

Step 2: Input Validation (Layer 0)

Purpose: Quick quality checks before heavy processing

What it checks:

- Is the image clear enough? (not too blurry or dark)
- Is GPS location available and accurate?
- Is the file valid and not corrupted?
- Is the photo recent? (not months old)

If failed: User gets immediate feedback like 'Photo is too blurry, please retake' or 'Please enable location services'

Step 3: Parallel Processing (Three Engines Work Together)

Once basic validation passes, three independent systems process the report simultaneously:

Engine A: AI Image Analysis

What it does:

- Identifies if the image shows a pothole or garbage
- Checks if the issue is actually visible in the photo
- Assesses severity (small, medium, or large problem)
- Detects landmarks in the photo to verify location
- Validates photo metadata (timestamp, camera info)

Output: AI Confidence Score (0-100)

Example: Photo clearly shows a large pothole → AI gives 92/100 score

Engine B: Fraud Detection

What it checks:

- **GPS Spoofing:** Did the user jump 100km in 2 minutes? (impossible travel)
- **Duplicate Reports:** Was this same issue already reported within 30 meters in the last 14 days?
- **Spam Patterns:** Is the user submitting 20 reports in one hour?

Actions:

- GPS spoofing detected → Major penalty (-50 points)

- Duplicate found → Link to original report, don't create new one
- Spam pattern → Flag for investigation

Engine C: Community Verification

How it works:

5. System finds users within 500 meters of the report location
6. Sends them a notification to verify the issue
7. Users vote: Yes (issue exists) or No (false report)
8. Votes are weighted (trusted users count more than new users)
9. After 3+ votes or timeout (6-48 hours), community score is calculated

Important: If no users are nearby (rural area) or timeout happens, the report continues anyway! Community verification is optional, not required.

Output: Community Confidence Score (0-100) or N/A if no votes

Engine D: Trust & History Check

What it analyzes:

- **User Reputation:** How old is the account? How many successful reports? Any fake report history?
- **Location History:** Have problems been reported here before? Is this a known problem area?
- **Past Patterns:** Does the user's behavior look normal or suspicious?

Output: Trust Score (0-100)

Step 4: Cross-Signal Validation

Now the system checks if all the signals are consistent with each other:

- **Location Consistency:** Does GPS say Liberty Chowk while AI detected Packages Mall landmarks 5km away? → Red flag!
- **Temporal Consistency:** Is the photo timestamp 3 days old but GPS reading fresh? → Suspicious!
- **Content Consistency:** User claims pothole but AI sees clean road? → Major conflict!

Bonus: If all signals agree (GPS, AI landmarks, and community all say same location within 100m) → +30 bonus points!

Step 5: Final Confidence Score Calculation

Formula:

Final Score = (AI Score × 40%) + (Community Score × 30%) + (Trust Score × 30%) + Bonuses - Penalties

Special Case: If community score is N/A (no votes), the weights adjust automatically:

Final Score = (AI Score × 55%) + (Trust Score × 45%) + Bonuses - Penalties

Decision Based on Score:

Score Range	Action
85-100	✅ AUTO-VERIFY - Report immediately sent to municipal department. Blockchain record created.
60-84	⚠️ REVIEW NEEDED - Report goes to officer's review queue for manual approval/rejection.
0-59	❌ REJECT/FLAG - Report rejected. User notified with reason. Repeated failures may trigger investigation.

Blockchain Integration (Accountability Layer)

Blockchain entry is created **only after a report is verified** (Auto-Verified(score \geq 85) or Officer-Approved(84 \Rightarrow score \geq 60)).

What is stored on blockchain (on-chain):

- Complaint ID(exactly same as in database)
- Cryptographic hash of image
- Issue category
- Verification timestamp
- Location hash (privacy-preserving, approximate)
- Verification type (auto/officer approved)
- status

What is NOT stored on blockchain (off-chain):

- Actual image file
- User personal information
- Full GPS coordinates
- Community votes

SUBMITTED



PENDING (off-chain)



UNDER_REVIEW (off-chain, if needed)



VERIFIED    Blockchain Event #1 (Verified Proof)



ASSIGNED (off-chain)



IN_PROGRESS (off-chain)



RESOLVED    Blockchain Event #2 (Resolution Proof)



CLOSED (off-chain final state)

Real-World Examples

Example 1: Clear Pothole, Trusted User, Community Verified

- AI Score: 92 (pothole clearly visible in photo)
- Community Score: 85 (5 nearby users voted, 80% said yes)
- Trust Score: 80 (user has 1-year account, 15 successful reports)
- Bonuses: +40 (no GPS spoofing, no duplicate, trusted user, known problem area)


Calculation: $(92 \times 0.4) + (85 \times 0.3) + (80 \times 0.3) + 40 = 126.3 \rightarrow$ Capped at 100

Result:  **AUTO-VERIFIED** → Sent to blockchain -> Sent to department immediately

Example 2: Low-Adoption Area (No Community Votes)

- AI Score: 88 (garbage pile clearly visible)
- Community Score: N/A (timeout, no users nearby in rural area)
- Trust Score: 65 (regular user, this is a new location)
- Bonuses: +15 (no GPS spoofing, no duplicate)

Calculation: $(88 \times 0.55) + (65 \times 0.45) + 15 = 92.65$ (weights adjusted because no community)

Result:  **AUTO-VERIFIED** → **AI + Trust were sufficient!-> sent to blockchain -> to department**

Example 3: GPS Spoofing Detected

- AI Score: 80 (image looks genuine)
- Community Score: 75 (people confirmed the issue)
- Trust Score: 60
- Penalties: -50 (GPS SPOOFING detected - user was in Karachi 1 minute ago, now in Lahore!)

Calculation: $(80 \times 0.4) + (75 \times 0.3) + (60 \times 0.3) - 50 = 22.5$

Result:  **MANUAL REVIEW** → **Flagged for investigation despite good AI score**

How We Handle Every Edge Case

Edge Case	Our Solution
Low App Adoption (No Community)	Community verification is optional. If timeout (no votes), AI + Trust scores get higher weight and can still approve genuine reports.
Fake Coordinated Reports	Pattern detection identifies users who always vote together. New accounts have reduced vote weight (0.5x). AI checks if issue is actually visible in photo.
GPS Spoofing	Fraud engine detects impossible travel speeds (100km in 2 minutes). Major penalty (-50 points) applied. Even high AI scores can't overcome spoofing penalty.
Duplicate Reports	Automatic detection within 30m radius and 14-day window. Duplicates are linked to original report as confirmations instead of creating new entries.
Emergency Issues	Keywords like 'exposed wire', 'open manhole' trigger urgency boost (+20 points). Shorter community timeout (6 hours vs 48 hours). Lower approval threshold.
Conflicting Signals	If GPS says Liberty but AI detects Packages Mall landmarks 5km away, large penalty (-40) applied. Report goes to manual review for investigation.
New User, Genuine Report	Low trust score but high AI score. Goes to manual review where officer sees all context. One approval builds reputation for future auto-approvals.
Poor Quality Photo	Input validation catches severe issues (very blurry/dark) and asks user to retake immediately. Borderline cases get lower AI score but can still pass with strong community/trust.

Complete System Flow Diagram

This diagram shows how a report moves through the entire system:

