Mobile Anti-Theft & IMEI Verification System (MAVIS)

Complete Project Documentation

Submitted by:
Okasha Nadeem
CPO X GIAIC Intern

Abstract

“A secure, government-aligned system to reduce mobile phone theft, verify device ownership, and protect buyers in the second-hand market using IMEI-based tracking and verification.”

1. One-line summary (purpose)

Make mobile snatching economically irrational by blocking safe resale channels and enabling police to trap and prosecute offenders — while protecting legitimate buyers — using an IMEI-and-ownership system (demo with dummy data; production with telco/OEM/legal integrations).

---

2. The real idea (what police gave us)

- Register devices to people at point of sale (IMEI ↔ CNIC).
- Allow shopkeepers / buyers to verify IMEIs before buying.
- When a device is reported stolen (FIR), use the registry + verification flow to trace/rescue it.
- Use an admin interface for police to inspect device details by IMEI.

---

3. Key weaknesses in the raw idea (why it needed strengthening)

- **Instant resale**: thief sells immediately, defeating traceability.
- **Single OTP**: owner OTP alone can be coerced or forged.
- **IMEI tampering / parts market**: IMEI change or selling as parts bypasses checks.
- **Blocking too early**: immediate network block removes evidence and reduces arrest probability.
- **Shop bypass**: unregistered shops / street buyers will remain safe channels.
- **No operational procedures**: no trap/forensic workflow, no human review before FIR.

---

4. What we added — the smart system (summary)

Each item below is implemented/defined in our design and demo:

1. **Mandatory IMEI registration at purchase** (IMEI + CNIC).
2. **Ownership ledger** — immutable ownership history per IMEI.
3. **Dual confirmation transfer** — seller + buyer confirmations; OTP + biometrics (where possible).
4. **Cooling period (48 hours)** — transfer pending state to allow police intervention.
5. **Trap Mode (soft)** — keep device usable but log/signal resale attempts and network events to build evidence.
6. **FIR auto-trigger → police review** — event-driven alerts, human confirmation before filing.

7. **Registered shop requirement + compliance scoring** — shop onboarding, audit trail, incentives and penalties.
8. **Parts & repair registry** — register and scan replacement boards/parts to choke parts market.
9. **Audit log & rate-limiting** — immutable logs and anti-abuse controls (OTP/rate limits).
10. **Panic/duress code** — special OTP that silently alerts police while returning apparent success.
11. **Separation of apps & backends** — User App (citizen/shop), Admin App (police/sysadmin), distinct services for clearer roles and security.
12. **Demo safety** — use seeded dummy data, simulated OTP/FIR flows; production readiness preserved.

---

5. Why these strategies (short justification)

- **Remove resale incentive** (mandatory registration + shop compliance + parts registry) → theft becomes low reward.
- **Increase arrest probability** (trap mode + telemetry + shop alerts + FIR linkage) → theft becomes high risk.
- **Protect buyers** (verify before purchase, transfer cool-off) → reduces demand for stolen phones.
- **Prevent circumvention** (ownership ledger + multi-attribute fingerprinting) → IMEI tamper or parts resale are traceable.
- **Maintain legal defensibility** (CNIC binding, immutable logs, human review before FIR) → reduces wrongful actions and supports prosecution.
- **Make system adoptable** (phased approach, demo → pilot → telecom/OEM integrations) → practical rollout path.

---

6. POV flows — step-by-step (concise)

A. Citizen (owner)

1. Buy phone → IMEI scanned at POS → CNIC verification → device registered to owner.
2. If stolen → file report in app (creates “Suspected Stolen — Soft Trap” state).
3. If attempt to sell later → receives OTP (or panic code) to approve/reject transfer.
4. In dispute → police appeal channel & human review.

Decision points / protections

- Cooling period prevents immediate transfer.
- Panic code lets owner signal duress.
- Audit trail proves ownership.

B. Thief (attack surface & expected behavior)

Common attacker strategies and our counters:

- **Quick resale** → blocked by registered-shop requirement + cooling period; resale attempts log trap signals.
- **IMEI tampering** → multi-attribute fingerprint + telco anomaly detection flag clones.
- **Parts resale** → parts registry prevents turning device into untraceable components.
- **Keep offline** → offline reduces utility; any later network event is logged and flagged.
- **Forced OTP** → dual confirmation + biometric / panic code mitigations.

C. Shopkeeper (buyer of used phones)

1. Customer presents phone → shop scans IMEI via Shop App.
2. App shows status: Safe / Pending Transfer / Suspected Stolen.
3. If Safe → shop initiates transfer workflow (seller & buyer confirm; 48h cooling).
4. If Suspected → shop triggers police verification; if police confirm, sale is blocked and evidence logged.

Business incentives

- Verified badge increases buyer trust.
- Compliance reduces legal liability.

D. Police (investigator)

1. Monitor trap alerts (resale attempts on stolen IMEIs, SIM events).
2. Review compiled evidence (shop scans, SIM changes, ownership history).
3. Human review → create FIR (system generates record and links device & events).
4. Execute investigation with telco data (cell-tower logs) and shop logs.

Key capability

- Event-driven investigations shorten time to action; evidence packaged in system aids prosecutions.

E. System / Admin

- Manage shop registrations, merchant compliance, audits, and analytics.
- Operate seed data / simulation for demo.
- Provide escalation and appeals workflow.

---

7. Implementation notes (demo → production)

- **Demo**: Next.js (TS) frontends; Node/Express (TS) backend; MongoDB; seeded data; simulated OTP & FIR. All flows implemented but no telco/OEM integration.
- **Production additions**: NADRA CNIC API, telco/PTA blocking APIs, GSMA DeviceCheck, secure cloud (gov-cloud), HSM/KMS, SIEM and legal agreements.
- **Governance**: PPP recommended; police-owned operational authority or joint steering committee.
- **Legal**: enabling regulation required for mandatory IMEI at point of sale and shop compliance obligations.

---

8. Services & integrations (single-page summary — what and why)

Service / Integration	**Purpose (why used)**
NADRA (CNIC verification)	Legitimate identity binding for ownership & legal traceability.
Telecom Operators (Jazz, Zong, Ufone, Telenor)	SIM events, IMSI-IMEI joins, cell-tower logs, execute IMEI blocking when legally approved.
PTA / DIRBS integration	National device registry alignment and enforcement; block unregistered/illegal IMEIs.
GSMA DeviceCheck / Global blacklist	Cross-border stolen device checks and international data sharing.
SMS / OTP gateway (Twilio or local provider)	Secure OTP delivery, panic code delivery, status notifications.

Service / Integration	**Purpose (why used)**
Cloud infrastructure (GovCloud / secure provider)	Scalable hosting with compliance (data sovereignty).
KMS / HSM	Secure key management for encryption, signature, and audit integrity.
SIEM / Logging (ELK, Datadog)	Centralized monitoring, anomaly detection, and forensic trails.
Analytics / BI (Mixpanel/Grafana)	KPI dashboards, hotspot detection, compliance reporting.
Parts & Repair Scanning APIs	Track serials of replacement boards to stop parts market.
NLP / AI fraud signals (optional)	Risk scoring, suspicious chain detection for prioritized police action.
FIR / Police case management system	Bi-directional linkage for automatic evidence attachment and legal workflows.
GSMA / OEM cooperation (Phase 3)	Activation locks, hardware-backed ID, hard IMEI block coordination.

Legal & policy dependencies: MoUs / SLAs required for telco, NADRA, PTA and police system integrations; data-sharing agreements and privacy safeguards must be established before telecom/OEM features go live.

---

9. Minimum demo deliverables to present (what to show)

- Registered device record + ownership timeline (JSON sample).
- Demo flow: register → report stolen → simulated resale attempt → trap alert → police review.
- Shop scan UI showing flagged device.
- Transfer workflow with dual confirmation and 48-hour pending state.
- Admin dashboard showing trap alerts and FIR stub.
- Task checklist summary (T001–T105) with completed items ticked.

---

10. KPIs (what the project will measure in pilot)

- Theft reports vs. recovered devices (target +x2 recovery).

- Reduction in street snatching over 12 months (target 30–50%).
- % of second-hand sales processed via registered shops.
- Mean police review time after alert (target ≤24 hours).
- Shop compliance rate.

---

11. Final operating recommendations (short)

1. **Pilot**: 6 months in a defined Karachi district with selected shops and police squad.
2. **Legal**: fast-track enabling regulation for IMEI registration and shop obligations.
3. **Ops**: dedicated police integration cell and shop onboarding team.
4. **Privacy**: store hashed CNIC, encrypted sensitive data, human review before FIR.
5. **Scale plan**: phase telecom integrations (6–18 months), OEM cooperation (18–36 months).

---

12. Existing IMEI-Based Anti-Theft and Verification Systems

Several governments and industry bodies have established systems or services that use IMEI information to prevent theft, verify device legitimacy, or assist citizens and authorities. These existing systems serve as real-world references and partial precedents for the MAIVS concept.

1. Pakistan — DIRBS (Device Identification, Registration & Blocking System)

Operator: Pakistan Telecommunication Authority (PTA)
Overview:
DIRBS is Pakistan's national IMEI registry and enforcement platform. It registers devices operating on local networks, blocks unregistered and illegal IMEIs, and includes functionality for reporting lost or stolen devices through its Lost & Stolen Device System (LSDS).
Key Capabilities:

- Central device registry
- Network-level blocking of illegal/unregistered/stolen devices
- Integration with telecom operators for enforcement
  Limitations (relative to MAIVS):
- Does not include shop verification workflows
- No structured ownership transfer or cooling period logic

2. Pakistan (Punjab) — e-Gadget

Operator: Punjab Information Technology Board (PITB) & Police
Overview:
e-Gadget focuses on used-device verification at the point of sale. Registered mobile shops use the system to log every sale with the buyer's identity (CNIC, photo) and scan IMEIs. If a phone is linked to a stolen device database, the system alerts the shopkeeper and police.
Key Capabilities:

- Retailer registration and compliance logging
- IMEI verification before resale
- Alerts for potentially stolen devices
  Limitations (relative to MAIVS):
- Coverage is regional rather than national
- No ownership transfer protocols with cooling periods
- Not a complete anti-theft lifecycle system

---

3. India — CEIR (Central Equipment Identity Register)

Operator: Department of Telecommunications (DoT), Government of India
Overview:
CEIR is a centralized national IMEI database that integrates carrier network data to block stolen or lost phones across service providers. Citizens can report devices as lost or stolen through the Sanchar Saathi portal or app. Blocked IMEIs are prevented from accessing the network, and recovery is facilitated when phones are found.
Key Capabilities:

- Unified IMEI registry across carriers
- National blocking of reported stolen/lost devices
- Citizen reporting via web and app portals
  Limitations (relative to MAIVS):
- No structured resale/control flow at point of sale
- Does not include shop compliance scoring or ownership transfer management

---

4. Global / Industry Collaboration — GSMA DeviceCheck

Operator: GSMA (Global System for Mobile Communications Association)
Overview:
DeviceCheck is a global initiative where participating mobile network operators share IMEI status (lost/stolen/blocked) to help prevent cross-border resale of stolen devices. Device status lookup is available to carriers and authorized parties.
Key Capabilities:

- Shared global IMEI status database
- Helps networks and authorized third parties check device legitimacy
  Limitations (relative to MAIVS):
- Primarily a lookup service, not a full anti-theft system
- No explicit police or shop compliance components

---

5. United States — Stolen Phone Checker (CTIA)

Operator: CTIA (Wireless Carrier Trade Association)
Overview:
The Stolen Phone Checker enables consumers and businesses to lookup whether an IMEI has been reported lost or stolen on participating U.S. carrier networks.
Key Capabilities:

- Consumer and business IMEI status lookup
  Limitations (relative to MAIVS):
- No ownership transfer or resale control
- Not integrated with police case management

---

6. Canada — DeviceCheck.ca

Operator: Canadian Telecommunications Association
Overview:
DeviceCheck.ca allows citizens, retailers, and law enforcement to check stolen device status within Canada's national IMEI database. It helps retailers avoid accepting stolen phones and assists investigations.
Key Capabilities:

- Stolen/lost IMEI lookup
- Retailer usage support
  Limitations (relative to MAIVS):

- No full ownership transfer or cooling period logic
- No shop compliance monitoring

---

7. OEM Device-Level Lock Systems

Operators: Apple, Google, Samsung (Global)
Examples:

- Apple Activation Lock
- Google Find My Device
  Overview:
  OEM-provided security features that make a phone unusable without the original account credentials, protecting a device from use after theft.
  Key Capabilities:
- Device-level activation locks
- Remote lock/wipe through OEM services
  Limitations (relative to MAIVS):
- Not part of a national IMEI registry
- Not integrated with law enforcement or resale verification workflows

---

Summary of Existing Systems vs. MAIVS

System	IMEI Registry	Theft Blocking	Shop Verification	Ownership Transfer	Police Integration
DIRBS (Pakistan)	Yes	Yes	No	No	Partial
e-Gadget (Punjab)	No	No	Yes	No	Partial
CEIR (India)	Yes	Yes	No	No	Yes
GSMA DeviceCheck (Global)	Yes (shared)	Lookup	No	No	No
Stolen Phone Checker (USA)	Yes	Lookup	No	No	No

System	IMEI Registry	Theft Blocking	Shop Verification	Ownership Transfer	Police Integration
DeviceCheck.ca (Canada)	Yes	Lookup	No	No	Partial
OEM Locks (Global)	No	Device	No	No	No

Key Insight

While several countries and organizations have **components of an IMEI-based anti-theft ecosystem**, none of them — including DIRBS, e-Gadget, CEIR, DeviceCheck, or OEM lock systems — combine all the following in a single workflow:

- Mandatory IMEI registration at purchase
- Usage of CNIC/identity binding
- Shop compliance and verification scoring
- Dual-OTP and cooling period ownership transfer
- Trap mode for resale attempts
- Police workflow with FIR linkage and evidence packaging
- Parts and repair registry
- Audit trail and anti-fraud analytics

MAIVS uniquely integrates all of the above into a unified national anti-theft and device ownership platform.

Appendix — One-line demo data examples

- Device: {"imei":"356789102345678","model":"Galaxy S22","owner":"OWN123","status":"Registered"}
- Owner: {"owner_id":"OWN123","name":"Ali Raza","cnic":"42101-1234567-1"}
- FIR: {"fir_id":"FIR-2025-0012","imei":"356789102345678","status":"Under Review"}