

TECHNICAL PRESENTATION | CYBERSECURITY

AI-Powered Detection of Malicious .in Domain Names

Protecting India's Digital Future

FOCUS AREA

Domain Threat Intelligence

APPROACH

4-Layer AI Detection Engine

SCOPE

.in ccTLD → Global TLDs

The Threat Landscape

- **3,000 new .in domains** are registered every single day
- Fraudulent sites mimic trusted brands — banks, e-commerce, government portals
- Manual detection is **reactive, not preventive** — victims are already harmed by the time a report is filed
- Scammers operate in cycles: **launch, steal, disappear, repeat**

Why Traditional Methods Fail

- Human review **cannot scale** to thousands of daily registrations
- Reporting-based takedowns average **days of lag time**
- During that window, **hundreds of users** are compromised
- Fraudulent sites are **visually indistinguishable** from legitimate ones

The AI-Powered Solution

A four-layer detection engine that activates **at the moment of registration**:

LAYER	METHOD	SIGNAL DETECTED
1	Domain Name Analysis	Suspicious patterns, brand impersonation
2	Network Graph Analysis	Coordinated bulk registrations
3	Content Inspection	Cloned UIs, credential harvesting forms
4	Behavioral Monitoring	Unusual traffic, redirection chains

Real-Time Detection Pipeline

DETECTION TIMELINE — FROM REGISTRATION TO BLOCK

- 9:00 AM → Malicious domain registered
 - 9:01 AM → AI flags: brand impersonation + cloned content detected
 - 9:02 AM → Alert issued — authorities notified automatically
 - 9:30 AM → Domain blocked — threat neutralized
- ✓ Zero users compromised

Proven Results

24,000

Fraudulent websites
detected in 6 months

<1 hr

Majority flagged within
1 hour of creation

2M+

Users protected from
potential fraud

CASE STUDY

143 fake SBI websites were identified and neutralized before a single victim was targeted — a testament to the power of proactive, AI-first detection.

Road Ahead

- **Pre-registration detection** via suspicious pattern analysis
- Expansion **beyond .in** to global TLDs for broader coverage
- **Cross-border collaboration** for international threat coverage
- Continuous model improvement as **adversarial tactics evolve**

Strategic Value

- Shifts cybersecurity posture from **reactive to proactive**
- **Scalable** — no linear increase in cost with domain volume
- Protects **brand trust** for businesses and public confidence in digital infrastructure
- Aligns with India's broader **digital safety and financial inclusion** goals

Closing Statement

“

Every fake website caught is someone's savings protected, someone's identity kept safe, someone's trust in the internet preserved.

**The internet should be safe for everyone.
AI makes that possible — one domain at a time.**