YOKTHA®
info@yokthatechnologies.com
Road Number 1, Kukatpally, Hyderabad, Telangana 500090, +91 96525 32753,

AI-POWERED FRAUD DETECTION FOR PAYMENT TERMINALS

The Problem · The Solution · The Impact

A Technical Overview of Hardware-Integrated AI Security Architecture for Point-of-Sale Infrastructure

01 | THE SCALE OF THE PROBLEM

India's payment infrastructure is under escalating attack. As digital transactions expand at unprecedented speed, fraudsters have evolved from software-based attacks to sophisticated physical tampering of payment terminals — exploiting a critical gap that software security alone cannot address.

₹48,021 Cr	46.4%	7.1%	$780M
Banking fraud value FY2025-26 — RBI	YoY rise in fraud value — RBI 2026	India fraud rate vs 3.8% globally	Global POS skimming losses 2025

Sources: RBI Annual Report 2025-26 · TransUnion Fraud Trends June 2026 · Coin Law 2025

Additional indicators confirm the urgency:

- UPI fraud incidents rose 85% in FY2024 — National Payments Corporation of India (NPCI)
- Cybercrime incidents increased from 10.29 lakh in 2022 to 28 lakh in 2025 — Government data
- Bluetooth-enabled skimming devices increased by 33% year-over-year in 2025
- India operates over 260,000 ATMs and millions of POS terminals — most with software-only fraud detection
- Most ATM and POS attacks in India still require direct physical contact with the terminal

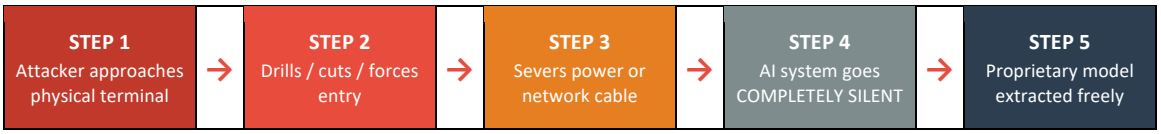
> *"Fraudsters are moving upstream — increasingly exploiting vulnerabilities at account creation and login, concealing identity manipulation until losses increase. — Anurag Anand, TransUnion India, June 2026"*

02 | THE CRITICAL VULNERABILITY

The fundamental weakness in current payment terminal security is not the AI fraud detection model itself — it is what happens to that model when the surrounding hardware is physically attacked.

YOKTHA®
info@yokthatechnologies.com
Road Number 1, Kukatpally, Hyderabad, Telangana 500090, +91 96525 32753,

How a Physical Attack Silences AI Fraud Detection



The 5-Step Physical Attack — no software-based system can defend against Steps 3–5

The consequences of this vulnerability:

- ✕ **No** alerts generated — the AI system cannot report what it cannot detect
- ✕ **No** forensic evidence preserved — transaction logs are inaccessible or destroyed
- ✕ **No** protection for proprietary AI models — algorithms extracted and replicated
- ✕ **Regulatory** non-compliance — RBI mandates continuous fraud monitoring availability
- ✕ **Financial** exposure window — attackers operate undetected until manual discovery

> *The core insight: Software security systems depend on power and network connectivity to function. A physical attacker simply eliminates both — and the entire AI defense layer collapses.*

03 | THE SOLUTION: HARDWARE-INTEGRATED AI SECURITY

The solution reframes the hardware enclosure — not as a passive container surrounding the AI system — but as an active extension of the AI system itself. When hardware and AI work together as a unified defense mechanism, physical attacks trigger the AI rather than silence it.

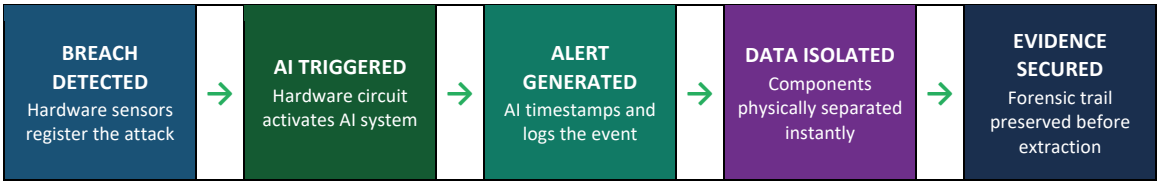
Our new product is Protected by **German Approved Patent** from industry experts on banking and financials.

Three Core Architectural Innovations

INNOVATION 1	INNOVATION 2	INNOVATION 3
Physical Compartmentalization	**Tamper-Responsive Circuit**	**Dual-Path Thermal Routing**
AI compute, storage, sensors & comms physically isolated into protected zones	Physical breach triggers AI alert independently of power or network state	Dedicated airflow channels keep AI processors cool under continuous operation

YOKTHA®
info@yokthatechnologies.com
Road Number 1, Kukatpally, Hyderabad, Telangana 500090, +91 96525 32753,

How Hardware-AI Integration Changes the Attack Outcome



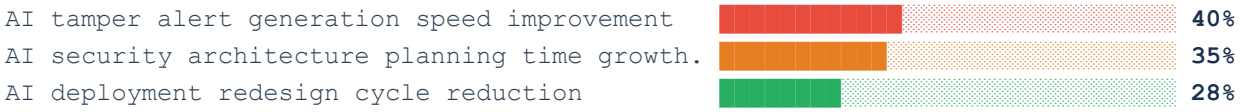
Hardware triggers AI — AI captures evidence — Response happens before any extraction can occur

> *Key breakthrough: The hardware-AI response operates completely independently of network connectivity or external power supply — the two attack vectors that defeat all software-only systems.*

04 | MEASURED OUTCOMES

Independent evaluation by an AI payment terminal company with enterprise banking background confirmed the following measurable improvements following adoption of this architecture:

Performance Improvements vs Previous Software-Only Approach



These improvements translate directly into reduced fraud exposure window, faster incident response, and stronger regulatory compliance posture across deployed payment terminal networks. In practical terms, a 40 percent faster AI alert generation speed means financial institutions can detect and respond to physical tampering attempts significantly earlier — closing the critical window during which attackers currently operate undetected. A 35 percent reduction in security architecture planning time directly lowers the engineering cost of deploying AI-integrated payment terminals at scale — making robust hardware-AI security accessible to a broader range of financial institutions and payment processors. A 25 to 30 percent reduction in redesign cycles accelerates the path from prototype to production deployment — enabling faster rollout of secure AI payment infrastructure across banking branches, retail environments, and public-facing transaction points. For financial institutions operating under Reserve Bank of India mandates for continuous fraud detection availability and operational resilience, these efficiency gains are not merely technical improvements — they represent a measurable strengthening of regulatory compliance posture and a direct reduction in the financial exposure associated with physical tampering attacks on AI-enabled payment systems.

YOKTHA®
info@yokthatechnologies.com
Road Number 1, Kukatpally, Hyderabad, Telangana 500090, +91 96525 32753,

05 | INDUSTRY-WIDE SIGNIFICANCE

The implications of hardware-integrated AI security extend far beyond any single deployment. Applied at banking sector scale, this architecture represents a structural shift in how the industry protects AI fraud detection systems at the hardware level.

Scale	India operates over 260,000 ATMs and millions of POS terminals — the overwhelming majority relying on software-only fraud detection vulnerable to physical tampering.
Regulatory	The Reserve Bank of India has increasingly mandated stronger fraud detection and operational resilience standards for payment infrastructure. This architecture directly enables compliance at the hardware level.
Financial Impact	A 40% improvement in AI alert generation speed applied across a major bank's nationwide terminal network would represent a transformational reduction in physical fraud exposure across thousands of terminals.
Global Relevance	With $780 million lost to POS skimming globally in 2025 and AI fraud detection being deployed at accelerating pace worldwide, the architectural principles represent a structural shift — not incremental improvement.

This is not incremental improvement. It is a structural shift in how AI fraud detection is protected at the hardware level.

For Product enquiries, orders, demo

Reach out to:
info@yokthatechnologies.com
+91 96525 32753