

Harish Sharma

Founder & CEO, Cipher Academy

Security architect · applied-AI engineer · information-warfare researcher

prin@cipher.academy | Delhi, India | cipher.academy | linkedin.com/in/prinsharma | github.com/Prinsharma1999

Professionally known as **Prin Sharma**. Portfolio: prin.cipher.academy

Summary

I break things, report them, and then build the fix. Offensive-security practitioner since 2018 and founder of Cipher Academy, a cybersecurity training company teaching iOS exploitation, hardware hacking and bug-bounty methodology. Seven years as security architecture lead on a large-scale analytics program. Builds and ships production AI end to end, and researches how coordinated inauthentic behaviour is detected and where detection breaks down.

Core Expertise

Offensive Security Hardware security · RFID / SDR / radio & telecom · iOS & Android security · mobile instrumentation (Frida, Objection) · web application security · Burp Suite · reverse engineering · red teaming · bug bounty

Security Architecture Threat modeling · hardening & access-control standards · OPSEC · OSINT · coordinated-behaviour detection · platform integrity

Applied AI LLMs & RAG · ASR / speech (Whisper, MLX, LoRA) · NLP · adversarial ML · knowledge graphs · PyTorch · Hugging Face Transformers

Engineering & Leadership Python · TypeScript · Swift · Kotlin · FastAPI · Next.js / React · PostgreSQL · DuckDB · Docker / Linux · team leadership · curriculum development · technical training

Professional Experience

Founder & CEO · Lead Instructor | Cipher Academy (registered MSME, Udyam) **Jan 2023 – Present**

- Founded and run a cybersecurity training company teaching real-world offensive security: iOS exploitation, hardware hacking and bug-bounty methodology, delivered to cohorts and B2B clients.
- Wrote and teach Buugsx, the flagship twelve-module bug-bounty course (web, mobile, AI/ML) with practice labs and a certification track; built the course platform and website.
- Authored three Udemy courses (Burp Suite, iOS security, NFT security), about \$10K in revenue over 2022–2024, retired as the material dated.
- Ship products under the Cipher Academy name: Graphlit / VIPL, Sayit, Bhāṣā Studio and NeuralGraph.

Independent Security Researcher & Consultant | Freelance **Jan 2018 – Present**

- Bug-bounty and red-team engagements across hardware, software and B2B targets; recognised in NordVPN's bug-bounty programme.
- Hardware, RFID, radio-frequency, telecom and SDR security testing on client devices and systems.
- Advise as an AI-plus-cybersecurity domain expert, with a focus on hardware security.

Security Architecture Lead | Strat News Global **Sep 2019 – Sep 2026**

- Owned the security architecture for a large-scale analytics program over seven years.
- Led a four-person team and worked alongside a 30+ person cross-functional group.
- Set the hardening, access-control and OPSEC standards used program-wide. Details under NDA.

Engineering Portfolio

- **Graphlit / VIPL** – sketch an app on a whiteboard and get a running application whose code is continuously verified against the drawing; 560+ commits; CLI and platform at graphlit.co.
- **Sayit** – phoneme-level pronunciation coaching; multi-tenant SaaS at sayit.cipher.academy that also runs fully offline from the same codebase; web and iOS.
- **Bhāṣā Studio** – self-hosted speech AI that transcribes, translates and dubs across India's 22 scheduled languages plus English (Whisper, NLLB, diarization, voice cloning, lip-sync).

- **NeuralGraph / StudyMe** – knowledge-graph engine for STEM learning; its first video pipeline rendered 100+ explainers across 1,400+ topics.
- **Media Monitor** – monitoring desk that watches every outlet in a source register (184 in its first deployment) and gives analysts a private workspace to read, annotate and export.
- **yτοςint & Sentinel** – coordinated-inauthentic-behaviour detection on YouTube (commenter overlap, burst and near-duplicate analysis on DuckDB) and an explainable disinformation threat-scoring engine.
- **NE & Neighbourhood News Tracker** – automated daily OSINT digest covering India’s North-East and neighbouring countries.
- **AVDA & Twix** – Android-emulator automation platform that runs device fleets in parallel through plugins, plus engagement analytics and monthly reporting.
- **India Defence Market Assessment** – citation-backed strategic advisory report, built as document-as-code (Markdown, matplotlib, Pandoc, XeLaTeX).
- **Bagri Dialect ASR** – Whisper fine-tuned with LoRA on Apple Silicon (MLX) for a Rajasthani dialect that has no Whisper language token.
- **Frida Workshop** – 14-script dynamic-instrumentation toolkit (SSL-pinning, root and anti-debug bypass) used in Cipher Academy’s mobile-security track.

Research & Publications

Self-published technical research through Cipher Academy on AI-era information operations, adversarial ML and platform integrity; about 20 papers, selected below. Full texts on request.

- **The Evasion Architecture** (Sep 2026) – ~97-page analysis of why algorithmic detection of AI-augmented coordinated inauthentic behaviour is failing: entropy, burst, graph-neural, LLM-text, perceptual-hash and deepfake detectors; information-theoretic bounds; a review across 73 elections; companion Legal & Regulatory Supplement (DSA, AI Act, FARA, GDPR).
- **Policy Gray Zones & the EU Regulatory Response** (Jul 2026) – DSA / AI Act / FARA gap analysis.
- **AI Microtargeting & Psychographic Targeting in Influence Operations** (Jun 2026).
- **Adversarial ML: AI Data Poisoning Against Training Pipelines** (May 2026).
- **Counter-CIB Technical Approaches** (Apr 2026) – survey of emerging detection methods.
- **CIB Effectiveness Analysis** (Mar 2026) – operational impact and the engagement paradox.
- **Cognitive Warfare & AI-CIB Doctrine** (Feb 2026).
- **Influence Operations: Deep Research** (Jan 2026) – landscape survey of state and commercial activity.

Recognition, Education, Languages & Interests

- **Recognition:** NordVPN bug-bounty programme, for responsibly disclosed security findings.
- **Education:** Self-directed in computer science, security and applied AI (left a Petroleum / Chemistry engineering program to pursue security full time).
- **Languages:** English (full professional), Hindi (native), Japanese (JLPT N5). **Interests:** Endurance cycling (200 km rides); specialty coffee.