



**MPHASIS AI & CYBERSECURITY
RESEARCH CO-LAB FOR
FINANCIAL SERVICES**



AI, DATA PROTECTION AND POST-QUANTUM CRYPTOGRAPHY (PQC)

WORKSHOP



18 - 19 JULY 2026



TECHNICAL REPORT

The workshop brought together regulators, top technical architects, senior technologists, and leading academics to examine the convergence of AI, data protection and post-quantum readiness in the BFSI sector.

DAY 1 – 18th JULY

Welcome Note and Introduction to the Workshop

Prof. Vadlamani Ravi

IDRBT



About the Mphasis Co-Lab

Prof. Sruthi Sekar

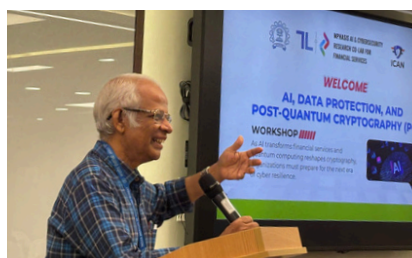
IIT Bombay



Opening Remarks

Prof. G. Sivakumar

IIT Bombay



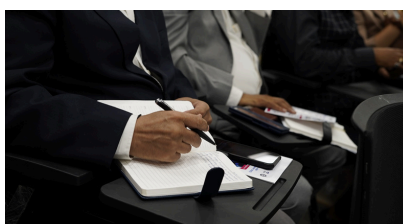
Key Themes

- Institutional Control** — Security expertise, architecture understanding and accountability must remain within the institution.
- AI Quality** — AI scales both capability and error; telemetry, labels, permissions and boundaries matter.
- Data Operations** — DPDPA connects data discovery, consent, retention, processors, rights and breach workflows.
- Crypto Agility** — Inventory and changeability come before any migration date or algorithm decision.
- Shared Capability** — Training, testbeds and industry-academia collaboration can widen access to specialist expertise.
- Privacy Engineering** — PET selection depends on the use case, trust boundary and privacy-utility trade-off.
- Last-mile Protection** — Users, identities, applications, APIs and suppliers form one connected attack surface.

Address By C-DAC Bangalore

Dr. Balaji Rajendran

C-DAC Bangalore





AI for Security and Security for AI

Prof. Sandeep Shukla

IIIT – Hyderabad



The dual role of artificial intelligence in cybersecurity spans both automated defensive capabilities and an expanded attack surface requiring dedicated security controls.

Defensive AI deployment encompasses automated alert triage, anomaly and real-time fraud detection, threat hunting, and controlled incident response. However, human-only defense pipelines are increasingly ineffective against machine-speed automated exploits, necessitating automated response mechanisms bound by explicit authorization limits and deterministic rollback boundaries.

Securing AI infrastructure requires protecting the full lifecycle: underlying models, prompt structures, training datasets, code repositories, inference pathways, supply chain dependencies, and autonomous agents granted system permissions. Key threat vectors include prompt injection, training data poisoning, model inversion, and compromised third-party model components. Operationalizing AI securely demands agent identity verification, least-privilege access execution, strict purpose-bound parameters, reproducible evaluation frameworks, and auditability.

AI FOR SECURITY	SECURITY FOR AI
Automated Alert Triage	Defense Against Prompt Injection
Real-time Fraud Detection	Training Data Poisoning Protection
Machine-Speed Response Loops	Model Supply Chain Auditing

DPDPA - 'Will it narrow the widening Digital Trust Deficit?'

Mr. Vittal Raj R

Member of the Expert Committee of RBI



Consent and purpose parameters must propagate across all system boundaries—including customer-facing channels, core banking platforms, analytical databases, marketing engines, and third-party processors.

- **Data Retention & Destruction Technicalities:**

- Enforcing retention limits requires automated cross-reconciliation across system logs, distributed backup environments, fraud ledgers, and legal hold records.
- Systems must automatically purge data upon purpose completion or consent withdrawal, except where explicit statutory retention mandates apply.

- **Non-Delegable Outsourcing Liability:**

- Financial institutions maintain full legal accountability for their third-party processor chains.
- Institutions must enforce complete processor visibility, compel auditability, verify immutable deletion logs, and establish coordinated incident response protocols.

- **Penalty Structures:** Clarified that monetary amounts listed under the DPDPA represent legal maximum ceilings for extreme non-compliance rather than standardized minimum fines.

Fireside Chat - Securing Digital Payments at Scale

Mr. Dilip Asbe

NPCI

Mr. Rajeev Agrawal

Innoviti Technologies



Digital payment rails must be treated as critical national infrastructure, requiring security architectures that scale dynamically alongside rapid transaction growth.

- **The Dual Security Frontier:**

- Regulated Backend – Highly structured environment relying on strict server-side access controls, HSM protection, and central key management.
- Consumer Last Mile – Highly unpredictable environment vulnerable to compromise via unpatched mobile operating systems, rogue application spaces, and psychological manipulation (social engineering).

- **Technical Enforcement of Data Rules:** Privacy parameters, such as explicit purpose specification and minimized data collection, must be enforced directly through software code rather than relying on policy documentation.

- **Device-Level Defense Standards:** Core application controls require strict OS isolation, detection and blocking of rooted/jailbroken devices, and robust key management.

- **Preparing Infrastructure for PQC:**

- Constructing detailed inventories of all active cryptographic keys and algorithms.
- Upgrading KMS platforms and HSM units to support post-quantum mathematical standards.
- Enabling flexible algorithm support and accelerating automated key rotation cycles.
- Running hybrid operational modes that blend classical encryption (e.g., AES/RSA) with new quantum-safe algorithms.

- **Compliance as Code:** Transitioning from manual, periodic regulatory audits to "compliance as code"—where compliance requirements are embedded directly into software pipelines for continuous automated enforcement.

Panel 1: Privacy by Architecture: PETs, AI and DPDPA-Ready Enterprises

Mr. Vikas Chaurasia

MeitY

Mr. Pravin Kumar

NPCI

MODERATOR

Prof. Manoj Prabhakaran

IIT Bombay

Mr. G. T. Venkateshwar Rao

POSIDEX

Mr. Hirak Mukherjee

XAFE AI



Traditional encryption protects data at rest (in storage) and in transit (over networks). Privacy-Enhancing Technologies (PETs) – advanced cryptographic and architectural methods used to process, analyze, and share data without exposing sensitive underlying personal information – protect data in use, that is, while being actively processed in memory.

- **Evaluating PET Implementations:** Technology selection is context-dependent and requires trade-off analyses across computational latency, storage footprint, processing overhead, data utility, and operational trust boundaries.
- **Foundational Governance Obligations:** Advanced cryptography does not replace core data management. Automated data discovery, precise purpose attribution, complete processor tracking, and data subject rights management remain mandatory operational requirements.

Panel 2: PQC Migration – from CBOM to a Crypto-agile BFSI

Dr. Ashutosh Bahuguna

CERT-In

Mr. Prasad Nambiar

IFTAS

MODERATOR

Dr. Balaji Rajendran

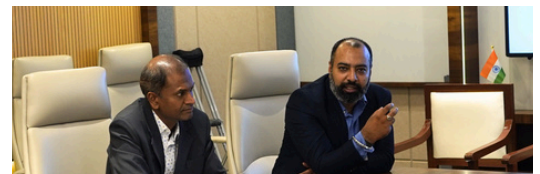
C- DAC Bangalore

Dr. Paras Arora

Mphasis

Mr. Adarash Trivedi

SEBI



Migrating financial infrastructure to post-quantum standards requires comprehensive planning and execution of complex technical changes

- **Establishing a Cybersecurity Bill of Materials (CBOM)**

- A CBOM is a comprehensive, structured inventory of all software components, hardware assets, cryptographic algorithms, certificate chains, and key lengths utilized within an enterprise ecosystem.
- Establishing a CBOM requires institutions to discover, catalog, and categorize all active cryptographic implementations across legacy applications, cloud microservices, payment gateways, and hardware devices.

- **Building Crypto-Agility**

- Crypto-Agility refers to the structural ability of an IT system to swap out cryptographic algorithms, keys, or protocols without disrupting the code or workflows.
- Will require decoupling hardcoded cryptographic algorithms from core application business logic using abstraction layers and APIs.
- Need to transition to central, flexible Key Management Systems that allow seamless algorithm upgrades.

- **Supply Chain Auditing**

- Institutions must consult thorough security audits of vendor software, embedded libraries, and third-party APIs to ensure safety and reliability, and post-quantum readiness across external software dependencies.

Panel 3: AI Threats & Opportunities in BFSI – Relevance of AI, Deepfakes, Adversarial ML & GenAI-driven Fraud

MODERATOR

Mr. Sachin Deodhar

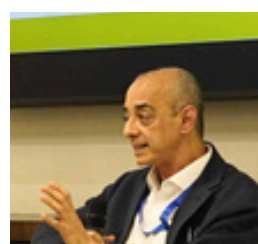
Sentinel Advisors

Mr. Bhargav Bhikkaji

MajorDomo Inc.

Mr. Krishna Sastry Pendyala

Cybersecurity Expert



Threats

- **Combating Shadow AI & Unmonitored Data Leakage:** Institutions must deploy robust network-level visibility and boundary inspection to identify unsanctioned external AI tools and stem unmonitored cross-border data exposure.
- **AI SOC Vulnerabilities & Telemetry Degradation:** Automated security models risk failing when trained on poor event logs or unverified telemetry, which yields inaccurate risk assessments and leads to flawed automated response actions.

Opportunities

- **Comprehensive AI Asset Governance & Control:** Institutions must establish end-to-end governance structures to systematically manage and secure AI agents, model parameters, prompt repositories, execution logs, and data pipelines.
- **Advanced Telemetry & Data Quality for AI Automation:** AI will help strengthen real-time security verification by validating underlying telemetry and training data labels to ensure accurate, high-fidelity threat detection.

Keynote Address - "Deconstructing AI Challenges in Cyber Security"

Mr. Avneesh Pandey

Securities and Exchange Board of India - SEBI



- **The Evolving Financial Attack Surface**

- Identity Layer: Exploitation of stolen valid credentials and sophisticated multilingual phishing campaigns.
- Device & Application Layer: Unauthorized rogue investment mobile apps and unmonitored mobile operating system exposures.
- Cloud & API Layer: Undocumented shadow API endpoints and opaque software third-party dependencies.

- **Defensive Action Plan:**

- Accelerating routine patching cycles and deploying virtual patching for legacy environments where underlying software modifications are constrained.
- Driving DevSecOps integration alongside continuous vulnerability exposure management.
- Deploying AI-assisted SOC and SOAR (Security Orchestration, Automation, and Response) workflows backed by auditable human oversight.

- **Leveraging Shared Infrastructure:** Expanding centralized Market-SOC capabilities to provide smaller market entities with high-grade security monitoring and threat intelligence.

- **Exploitability-Based Prioritization:** Shifting vulnerability management research from counting raw vulnerability numbers to ranking findings based on real-world exploitability and active threat exposure.



Way Forward & Roadmap

Prof. G. Sivakumar

IIT Bombay



Closing Note | Online

Prof. Ashok Jhunjunwala

ITEL Foundation / IIT Madras



Non-Delegable Institutional Accountability

Financial institutions must accept that ultimate responsibility for cyber resilience rests solely on their shoulders. While outsourcing to third-party software vendors and cloud providers offers operational efficiency, it does not absolve institutions of their legal or operational risk. They cannot transfer their core compliance obligations outward, meaning leadership must maintain rigorous oversight and continuous risk management across all vendor ecosystems.

Sustained Industry-Academia Bridges

To stay ahead of evolving threats, the financial sector needs structured, ongoing collaboration channels with academic researchers. By actively bridging the gap between theory and practice, institutions and universities can co-develop targeted skill tracks, tackle real-world security challenges, and significantly accelerate the pipeline that moves security tools from lab prototypes into live production environments.

DAY 2 – 19th JULY

OBJECTIVE

To bring together experts to deliberate on key cybersecurity priorities in the BFSI sector including DPDPA implementation, crypto-agility, and post-quantum readiness, and to develop actionable recommendations and a collaborative roadmap for strengthening cyber resilience across the BFSI sector.



Dr. Leeladhar Meena, Director (West), NCIIPC, led the discussions.

The session successfully formulated actionable recommendations and a collaborative roadmap to strengthen cyber resilience, advance technological indigenization, and deepen regulatory alignment across the financial sector.

OUTCOMES

- **BFSI Ecosystem Strengthening:** Advanced collaborative discussions with key regulatory bodies, including SEBI, to align security practices and enhance resilience across the BFSI sector.
- **Capacity Building & Training Roadmap:** Synthesized industry feedback on critical skill gaps to design a roadmap for upcoming, highly specialized hands-on workshops.
- **National Security & Sovereignty:** Initiated strategic dialogue on promoting indigenization and safeguarding India's digital sovereignty within critical security infrastructure.

ACTION POINTS

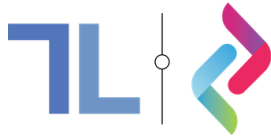
- **Central Problem Bank & Single Point of Contact (SPoC):** Maintain a repository for high-priority problem statements from agencies like NCIIPC, CERT-In, I4C, and NIA, matching them directly to vetted startups – Mphasis Co-Lab can help with creating and maintaining.
- **Multi-Tier Registries:**
 - a. **Academic Capability Registry:** Mapping expertise across member institutions.
 - b. **Curated Indian Startup Registry:** Filtering and vetting indigenous cybersecurity startups free from foreign control or simple white-labeling.
 - c. **Stakeholder & User Registry:** Connecting BFSI, government, and strategic sectors.
- **Targeted Working Groups & Reference Architectures:**
 - a. **Isolated Recovery Environment (IRE) Architecture:** Jointly developing a ring-fencing reference framework for critical assets with bank CISOs and NCIIPC.
 - b. **Cryptographic Bill of Materials (CBOM):** Developing minimum viable tools and guidance to map cryptographic dependencies across large enterprises.





MPHASIS AI & CYBERSECURITY RESEARCH CO-LAB FOR FINANCIAL SERVICES





**MPHASIS AI & CYBERSECURITY
RESEARCH CO-LAB FOR
FINANCIAL SERVICES**



THANK YOU !

Scan & subscribe to our social media
channels for regular updates



@iitb-mphasis-cybersecurity-colab-bfsi



trustlab@cse.iitb.ac.in



+91 8657947489



trustlab.iitb.ac.in



Department of Computer Science Engineering, IIT Bombay, Powai, Mumbai - 400076