Programme on

AI/ML for Cyber Security: Double Edge Sword

Programme Coordinator: Dr. Mridula Verma

FEBRUARY 23 - 27, 2026

INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY, HYDERABAD

(ESTABLISHED BY RESERVE BANK OF INDIA)

Introduction

As the adoption of Artificial Intelligence (AI) and Machine Learning (ML) accelerates in the banking sector, institutions face a double-edged reality: AI/ML technologies enable more intelligent, automated, and adaptive cyber defenses against increasingly sophisticated threats, while simultaneously introducing new and complex risks such as data privacy breaches, adversarial attacks, model vulnerabilities, opaque decision-making, and regulatory non-compliance. Although AI-driven systems promise significant gains in efficiency, resilience, and personalization, they also expand the attack surface across data, model, and infrastructure layers, requiring security-by-design, strong governance, and continuous risk oversight. With emerging regulations such as India's Digital Personal Data Protection Act (DPDPA) and heightened scrutiny from global regulators, banking professionals must develop a balanced understanding of how to responsibly deploy, secure, govern, and audit AI/ML systems. This Executive Development Programme equips mid-to-senior level banking professionals with a strategic and practical perspective on leveraging AI/ML to strengthen cybersecurity postures while effectively managing privacy, security, compliance, and governance challenges within the financial ecosystem.

Objectives

- Build a strong foundation in AI/ML concepts and their application in strengthening cybersecurity through intelligent threat detection, prediction, and response mechanisms.
- Identify and assess cyber, privacy, and security risks across the AI/ML lifecycle, including data collection, model development, deployment, and ongoing monitoring, using data-driven approaches.
- Analyze real-world banking use cases and emerging threats such as adversarial machine learning, model drift, and vulnerabilities in distributed and federated learning environments.
- Interpret and apply regulatory and ethical expectations for responsible AI, in alignment with DPDPA, RBI guidelines, and relevant global standards.

Contents

- **Foundations of AI/ML in Banking Cybersecurity and Risk:** AI/ML and cybersecurity fundamentals, BFSI threat landscape, data privacy principles, security challenges across the AI/ML pipeline, and responsible AI (ethics, fairness, accountability).
- **AI/ML for Threat Detection, Fraud, and Insider Risk:** Anomaly and intrusion detection, real-time fraud detection, and biometric and behavioral authentication.
- **Adversarial AI and Model Risk Management:** Adversarial machine learning (evasion and poisoning), explainable and robust AI, model monitoring and drift management, shadow AI risks

- **Secure AI Infrastructure Automation:** AI-enabled SIEM and SOAR automation, alert correlation and false-positive reduction, GenAI and NLP for playbooks and threat reporting, cloud and AI supply chain security, and DevSecOps for ML pipelines.
- **Governance, Compliance, and Strategic Implementation:** AI governance frameworks for banks, risk-based audit and compliance aligned with DPDPA, RBI, and global norms, organizational readiness, and emerging trends including GenAI and quantum-safe security.

Who can Participate?

Senior Executives (up to AGM level) and Junior Officers (up to SM level) from IT Divisions of Banks involved in technology, risk, customer experience, and strategic planning.

End Use

By the end of the Programme, participants will be able to critically evaluate the use of AI/ML in their institutions from both cybersecurity and risk-governance perspectives, make informed decisions on secure and compliant AI adoption, engage effectively with technology, risk, legal, and compliance teams, and provide strategic oversight on AI-enabled cybersecurity initiatives, governance frameworks, and regulatory alignment in banking environments.

Programme Coordinator

Dr. Mridula Verma, Asst. Professor. e-mail: vmridula@idrbt.ac.in.

Accommodation

Participants will be provided Air Conditioned Single Occupancy accommodation in IDRBT, Hyderabad, with all cafeteria facilities. The Participants can check-in on the evening of the day before the commencement of the programme and can check-out after completion of the programme on the same day (or) in the morning of the next day of the programme.

Fee Details

Domestic Participants from

- RRBs & Coop. Banks : Rs. 50, 000 + Applicable GST
- All other Banks & FIs : Rs. 65, 000 + Applicable GST

The fees for our programmes can be remitted through NEFT and the bank account details for fee payment are here under:

Account Name	:	IDRBT
Bank	:	Axis Bank Limited
Branch	:	Humayun Nagar (Mehdipatnam Ring Road) Branch,Hyderabad
Account Number	:	426010100018823
IFSC Code	:	UTIB0000426
GSTIN	:	36AAAAI0204K1Z4.

Nominations

Nominations may be sent by filling the ☞ *Nomination Form (click to fill the form)* latest by **FEBRUARY 07, 2026. Please note that no nominations will be accepted after this date**. This measure is envisaged to further improve the quality and learning outcomes of the programmes based on participants' profile and requirements.

While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No / Phone No., email address) along with the nominating authority details (Name, Designation, Bank, Mobile No / Phone No., email address, Fee billing address, GST No. of the bank).

Contact Us

Please contact our Programme Office for organizing Customized Programmes and/or any other queries related to programmes at **hunar@idrbt.ac.in** or call us on +914023294141/21.

Forthcoming Programmes of February 2026

S. No.	Programme	Date	Coordinator
1.	Intelligent Process Automation	02 - 06	Prof. V. N. Sastry & Dr. Mridla Verma
2.	Security, Scale and Access for Digital Payments (A Joint programme with NPCI)	04 - 06	Dr. Abhishek Thakur
3.	Quantum Computing	04 - 06	Dr. P. Syam Kumar
4.	Data Center Management – IT & Non-IT	09 - 13	Dr. Abhishek Thakur
5.	Containerization	09 - 11	Dr. P. Syam Kumar
6.	Customer Identity and Digital Personal Data Protection Compliance for Banks and Financial Institutions	11 - 13	Prof. V. N. Sastry
7.	Application Security & Dev-Sec-Ops	16 - 18	Dr. Abhishek Thakur & Dr. Dipanjan Roy
8.	Data Privacy and Cloud Security	16 - 20	Dr. P. Syam Kumar & Dr. Susmita Mandal
9.	End to End Implementation of AI/ML in Banking	16 - 20	Dr. V. Ravi
10.	Information Systems Controls & Audit	23 - 27	Dr. Dipanjan Roy
11.	AI/ML for Cyber Security: Double Edge Sword	23 - 27	Dr. Mridula Verma
12.	IT Supply Chain Risk Management	25 - 27	Dr. N. P. Dhavale

Please visit our website for more details on programmes at
https://www.idrbt.ac.in/executive-development-programmes/