



# Institute for Development and Research in Banking Technology

(Established by Reserve Bank of India)

Castle Hills, Road No. 1, Masab Tank, Hyderabad-57, India.

---

e-Programme on

## PRIVACY AND SECURITY RISKS IN MACHINE LEARNING

June 14 – 17, 2022

---

### Introduction

Machine learning is widely used today for solving problems in varied domains, including banking/finance, customer management, customer on boarding, document verification for e-KYC, identity verification, cyber security, Chatbot etc. In general, any data-driven process is benefitted by the developments in machine learning. But several privacy and security concerns have been raised, of late, related to these machine learning based approaches.

### Objective

The objective of this e-programme is to enlighten the participants about the privacy and security risks in machine learning based approaches.

### Contents

- Privacy preserving approaches for machine learning
- Adversarial attacks in machine learning (e.g., data poisoning, model stealing etc.)
- Mitigations against adversarial attacks

### Mode of Teaching

Online teaching plus learning inputs through reading material, videos, webinars, assignments, quizzes, online interactions and clarifications. Each e-Programme will have four live webinars and course material will be made available in advance for study.

### Who Can Participate?

Staffs from any department of banks (across various levels of hierarchy) can attend the program. Staffs from other financial organizations can also attend the program.

### End Use:

Knowledge about the privacy and security risks in machine learning will help the banks to adopt relevant practices to mitigate those risks at the time of building the machine learning based approaches.

### Programme Coordinator:

**Dr. Rajarshi Pal**, Assistant Professor, IDRBT;

e-mail: [prajarshi@idrbt.ac.in](mailto:prajarshi@idrbt.ac.in)

## Fees:

### **For Indian Participants**

- RRBs & Coop Banks: Rs. 11,800/- (Rs. 10,000/- + 18% GST)
- All Other Banks & Financial Institutions: Rs. 14,750/- (Rs. 12,500/- + 18% GST)

### **For International participants**

- US \$ 220 (per participant, All inclusive)

## Bank Account Details for Remittance of Fees

The fees for this e-programme can be remitted to the following accounts:

### **For Indian Participants**

Account Name : IDRBT  
Bank & Branch : Axis Bank Limited, Humayun Nagar, Mehdiapatnam, Hyderabad  
Account No. : 426010100018823  
MICR Code : 500211012  
IFSC Code : UTIB0000426

### **For International participants**

Receiver's Correspondent Bank : JP Morgan Chase, New York, USA  
Swift Code : CHASUS33XXX  
Fed Wire Routing Number : ABA 021000021  
Beneficiary Bank & Branch : Axis Bank Ltd., Mumbai, India  
Account Number : 0011407376  
Beneficiary Bank Swift Code : AXISINBB

### **Ultimate Beneficiary**

Account Name : IDRBT  
Customer ID : 030021632  
Account No. : 426010100018823  
Bank & Branch : Axis Bank Ltd., Jubilee Hills, Hyderabad, India. (AXISINBB030)

## Nominations

Banks may nominate any number of participants to these e-Programmes, which may be accepted on a first-cum-first-served basis. While nominating, please provide the details of the participants (Name, Designation, Bank, Mobile No/Phone No, email address, fees billing address, GST No. of the Bank).

Apart from nominations by banks, staff members of banks can self-nominate themselves for these e-Programmes by providing their employee credentials and paying the programme fee latest by **June 13, 2022**.

## How to Register

The nominations for these e-Programmes, and queries if any, may please be sent to [eprogram@idrbt.ac.in](mailto:eprogram@idrbt.ac.in). Please visit <https://www.idrbt.ac.in/eprogrammes> for more details about these programmes.

\*\*\*\*\*

## **e-Programmes in June 2022**

<b>S. No.</b>	<b>Name of the e-Programme</b>	<b>Date</b>	<b>e-Programme Coordinator</b>	<b>Last Date for Nomination</b>
1	Privacy Preserving Machine Learning for Banks	06 – 09	Dr. V. Ravi	<b>June 03, 2022</b>
2	Distributed Ledger Technology and Banking Applications	06 – 09	Dr. N. V. Narendra Kumar	<b>June 03, 2022</b>
3	5G Use Cases and IoT Applications for Banks	06 – 10	Dr. V. N. Sastry	<b>June 03, 2022</b>
4	Threats to Digital Payment Ecosystem	07 – 10	Dr. Susmita Mandal	<b>June 06, 2022</b>
5	Technologies for Financial Inclusion	07 – 10	Dr. M.V.N.K. Prasad	<b>June 06, 2022</b>
6	Emerging AI/ML Technologies	13 – 16	Dr. Mridula Verma	<b>June 10, 2022</b>
7	Workshop on Registration Authority Operations	14 – 17	Dr. N. P. Dhavale	<b>June 13, 2022</b>
8	Privacy and Security Risks in Machine Learning	14 – 17	Dr. Rajarshi Pal	<b>June 13, 2022</b>
9	RBI Guidelines on Cyber Security	20 – 23	Dr. Dipanjan Roy	<b>June 17, 2022</b>
10	Introduction to Containers	21 – 24	Dr. P. Syam Kumar	<b>June 20, 2022</b>
11	Targeted Attacks - Detecting in Early Stages	21 – 24	Dr. B. M. Mehtre	<b>June 20, 2022</b>
12	API Development	Jun 28 – Jul 01	Dr. V. Radha	<b>June 27, 2022</b>