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

MARCH 14 – 17, 2023

Introduction

Machine learning is widely used today for solving problems in varied domains, including banking/finance, customer management, customer onboarding, 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

The program will have four live webinars. One webinar will be held at each day of the program. Duration of each webinar will be one hour. Additional study materials will be made available in the form of text and video lectures. Participants can go through those materials offline.

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

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, Mehdipatnam, 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 **MARCH 13, 2023**.

How to Register

The nominations for these e-Programmes, and queries if any, may please be sent to *eprogram@idrbt.ac.in*. Please visit ***https://www.idrbt.ac.in/e-programmes*** for more details about these programmes.

*****

E-Programmes in March 2023

S. No.	Name of the e-Programme	Date	e-Programme Coordinator	Last Date for Nomination
1	Privacy and Security Risks in Machine Learning	14 – 17	Dr. Rajarshi Pal	**Mar 13, 2023**
2	Data Centre Management	14 – 17	Dr. P. Syam Kumar	**Mar 13, 2023**
3	Advanced Topics in Cyber Security	14 – 17	Dr. B. M. Mehtre	**Mar 13, 2023**
4	Continuous Security Validation	14 – 17	Dr. V. Radha	**Mar 13, 2023**