ARE DEEP LEARNING MODELS TRUSTWORTHY?
A Training Programme on Adversarial Attacks and Defence Techniques in Deep Learning Models

TARGETED AUDIENCE:
UG / PG STUDENTS/ RESEARCH SCHOLARS, FACULTY MEMBERS AND INDUSTRY PROFESSIONALS

14TH & 15TH JUNE 2024
ONLINE MODE

CONTACT:
Dr. V Mary Anita Rajam
Director, CCS
+91 44 2235 8829
+91 98407 00071

Last Date for Registration: 20 May 2024
About the Centre for Cyber Security:
The Centre for Cyber Security was established in April 2022 as a research centre under Anna University. Its focus is to excel in research and provide academic excellence in cyber security. The Centre for Cyber Security collaborates with the industry to take up consultancy and projects, offers value-added courses and training in the area of cyber security to improve the employability skills of students, and strives to discover security vulnerabilities and prevent hacking.

About the Department of Computer Science and Engineering:
The Department of Computer Science and Engineering was started in the year 1987. DCSE offers undergraduate, postgraduate and research programs in various disciplines of CSE. This department offers B.E. programme in Computer Science and Engineering and three M.E. programmes. The department promotes active industry-institute collaboration by identifying areas of interest and taking part in sponsored research projects and consultancy services both for the private and public sectors.

About the Training Programme:
The training programme includes the following topics:
- Introduction to Deep Learning (DL)
- Introduction to Convolutional Neural Networks
- Overview of Security Vulnerabilities in DL Models
- Overview of Interpretability Methods
- What are Adversarial Attacks?
- Existing Defence Mechanisms
- Interpretability and Defence
- Code Walkthrough

Fee details:

<table>
<thead>
<tr>
<th>Category</th>
<th>Registration Fee (inclusive of GST)</th>
</tr>
</thead>
<tbody>
<tr>
<td>UG / PG Student / Research Scholar</td>
<td>Rs. 944</td>
</tr>
<tr>
<td>Faculty members</td>
<td>Rs. 1180</td>
</tr>
<tr>
<td>Industry Professionals</td>
<td>Rs. 1770</td>
</tr>
</tbody>
</table>

Registration Link: [https://forms.gle/MwbfqYbdYL9QdSpj7](https://forms.gle/MwbfqYbdYL9QdSpj7)

The candidates have to upload their ID cards from their respective college/organization. The Programme has limited seats. The selected candidates will be intimated through e-mail. After the selection e-mail, payment for registration has to be made.