VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

One Day Hybrid Workshop on Adversarial AI and LLM Security: Red Teaming, Vulnerability Assessment and Defence

21st November 2026

Organized by

School of Computer Science and Engineering (SCOPE)

Vellore Institute of Technology

Vellore – 632014



Organizing Committee

Chief Patron:

Dr. G. Viswanathan, Chancellor

Patrons:

Dr. Sankar Viswanathan, Vice President

Dr. Sekar Viswanathan, Vice President

Dr. G.V. Selvam, Vice President

Dr. Sandhya Pentareddy, Executive Director

Ms. Kadhambari S. Viswanathan, Assistant Vice President

Co-Patrons:

Dr. V. S. Kanchana Bhaaskaran
Vice Chancellor

Dr. Partha Sharathi Mallick
Pro-Vice Chancellor

Dr. T. Jayabarathi, Registrar

Convener:

Dr. N. Jaisankar, Dean In-charge, SCOPE

Co-Convener:

Dr. H Parveen Sultana, Associate Dean In-charge, SCOPE

Organizing Secretaries:

Dr. R. Rajeshkannan
Head - Information Security
SCOPE

Dr. P. Gayathri
Head - Software Systems
SCOPE

Coordinators:

Dr. M. Thirunavukkarasan, Associate Professor
Department of Computational Intelligence
SCOPE

Dr. S. Ramani, Associate Professor Sr.
Department of Information Security
SCOPE

Contents of the Programme

- Introduction to Adversarial AI and LLM Security
- Fundamentals of Large Language Models and AI Threat Landscape
- Prompt Injection, Jailbreaking and Prompt Manipulation Attacks
- Adversarial Machine Learning and Data Poisoning
- Model Extraction, Evasion and Privacy Attacks
- AI Red Teaming and LLM Vulnerability Assessment
- Security of RAG-Based Applications and Autonomous AI Agents
- Defensive Strategies, AI Guardrails and Secure LLM Deployment
- Capture the Flag (CTF) Challenge – Hands-on AI Security Exploitation and Defence Competition

Target Audience:

Faculty members, Research Scholars, UG and PG students

Registration:

The participants are requested to register for the workshop through the following link

https://events.vit.ac.in/

Registration fee (Including GST): 200/-

Last date for registration: 19.11.2026

About VIT

VIT was established with the aim of providing quality higher education on par with international standards. It persistently seeks and adopts innovative methods to improve the quality of higher education on a consistent basis. The campus has a cosmopolitan atmosphere with students from all corners of the globe. Experienced and learned teachers are strongly encouraged to nurture the students. The global standards set at VIT in the field of teaching and research spur us on in our relentless pursuit of excellence. Our Memoranda of Understanding with various international universities are our major strength.

About SCOPE

The school has one of the best infrastructures including domain-specific labs associated with the technical departments. The main aim is to produce computing graduates with potential, to design and develop systems involving the integration of software and hardware devices, employ innovative approaches in programming and problem solving, and create Large Scale Software Systems. With an objective of developing core competence in the subject matter specializations and special interest groups for learning newer technologies.

Departments

The school has formed the following technical departments:

- Department of Analytics
- Department of Computational Intelligence
- Department of Database Systems
- Department of Software Systems
- Department of Information Security
- Department of IoT
- Department of Quantum AI

About Workshop

This workshop aims to provide an in-depth understanding of emerging security challenges associated with Artificial Intelligence (AI) and Large Language Models (LLMs), with a particular focus on adversarial attacks, vulnerability assessment, and defensive strategies. Participants will explore critical security threats such as prompt injection, jailbreak attacks, data poisoning, model manipulation, and adversarial exploitation of AI-powered applications. The workshop will introduce the principles and practical methodologies of AI red teaming, security testing, vulnerability identification, and risk mitigation to evaluate the robustness and reliability of intelligent systems. Through technical discussions and hands-on demonstrations, participants will gain insights into identifying vulnerabilities, assessing potential attack surfaces, and implementing effective defence mechanisms to develop secure, resilient, and trustworthy AI systems.

Resource Person Details

Mr. Dinesh Paranthagan
Founder & CEO
Hackup Technology Pvt. Ltd., Coimbatore

For further details contact:
Email: thirunavukkarasan.m@vit.ac.in,
ramani.s@vit.ac.in
Mobile: +91-9597394733
+91-9976590495

Participants are requested to register for the workshop through following web link

https://events.vit.ac.in/