PSG College of
Technology, Coimbatore

# Students Union 2024-25


***The Global Clash of Techno Talentz***

## KRIYA 2K25

## Event Resource Form

## Workshops

ASSOCIATION NAME : Computer Science & Engg Association

WORKSHOP NAME : ARC - AI-driven Resilient Cybersecurity

# INSTRUCTIONS

### (TO BE READ BEFORE FILLING THE FORM)

***** If two different events are to be conducted then fill the above form for each event separately and submit it.

****** If the same event continues on both the days (i.e.) Preliminary round on first day and final round on second day, then fill the needed requirement in the same form.

## Instructions:

1. Not all the events and workshops submitted will be approved.
2. Maximum of two events, one workshop, one paper presentation can be proposed.
3. Events and workshops should be innovative or based on the trending new technologies relating to the respective stream.
4. Judges must be present throughout the duration of event.
5. No cash prize / memento or any other form of prizes should be given by clubs/association to the event winners.
6. Names for the external guest should be provided by the Students Union if filled-in the items required table.
7. Certificates to the winners, runners, coordinators & volunteers of each event will be provided by the Students Union.
8. If any materials are required prior to the day of the event, please mention “Required in advance” near that material in the “Item Name” column.
9. Halls will be allocated on the basis of availability.
10. The projector will not be provided by the Students Union, use the projector available in the hall.
11. Winner and runner details should be submitted within one hour from the end of event.
12. HDMI cables / VGA converter will not be provided.
13. Take enough copies of the form, for your reference.
14. Further changes are not accepted.
15. Submit it to the point of contact allocated to your club/association.
16. For more details contact your respective point of contact.

Signature of the Secretary

Signature of the Faculty Advisor

# Workshop Preview: WKSP16

## Secretary Details

| Name | Roll Number | Mobile No |
|---|---|---|
| Mithilesh E N | 21Z229 | 8883912299 |

## Convenor Details

| Name | Roll Number | Mobile No |
|---|---|---|
| Arun U S | 22N208 | 8610250639 |
| Richard Samuel D | 22N242 | 9384559645 |

## Volunteer Details

| Name | Roll Number | Mobile No |
|---|---|---|
| Mehul Dinesh | 22N232 | 8608715000 |
| Lohith S | 22N228 | 9488125100 |

## Faculty Advisor Details

| Name | Designation | Contact Details |
|---|---|---|
| Dr. N. Gopikarani | Assistant Professor | 9994153301 |

## Speaker Details

| Name | Designation | Contact Details |
|---|---|---|
| Dhanush Gowdhaman | Software Engineer, IBM | 9535362134 |

## Signature of the Speaker

Workshop Details

**DAY 2** ● **DAY 3** ○ **BOTH DAYS** ○

EXPECTED NO. OF PARTICIPANTS: 50

PROPOSING FEES: 700

Justification: The speaker will conduct sessions on advanced cybersecurity and artificial intelligence topics.

SPEAKER REMUNERATION (if any)(With justification): 10000

Justification: general charge and travel expenses

NUMBER OF HALLS/LABS REQUIRED: 1

HALLS/LABS PREFERRED: 3AI Lab (E Block)

Reason:

DURATION OF THE EVENT IN HOURS: 6

START TO END TIME

SLOT 1 : 9:30 TO 12:30

SLOT 2 : 1:30 TO 4:30

| SLOT 1 | SLOT 2 | FULL DAY |
|---|---|---|
| ○ | ○ | ● |

No of Extension box: 1

Reason : for speaker

No of mic: 1

Reason : for speaker

Signature of the Secretary:

Signature of the Faculty Advisor:

## Items Required

| S.No. | Item Name | Quantity | Price per Unit | Total Price |
|---|---|---|---|---|
| 1 | Permanent marker (Black) | 1 | 0 | 0 |

# Workshop Details

## WORKSHOP NAME: ARC - AI-driven Resilient Cybersecurity

## WORKSHOP DESCRIPTION:

This workshop is designed to introduce you to the fascinating intersection of AI and cybersecurity, with a focus on both the theoretical underpinnings and hands-on implementation of core concepts. We'll dive into the latest trends and technologies, including: Generative AI for creating and detecting adversarial attacks. Federated Learning for secure, decentralized threat detection. Homomorphic Encryption to train machine learning models while preserving data privacy. Zero Trust Security Models powered by AI for adaptive, real-time threat detection. AI-based Firewalls like FLARE (Federated Learning and Resilient Encryption) for dynamic response to cyberattacks. Explainable AI (XAI) to build trust in security systems by making AI-driven decisions more transparent. Large Language Models (LLMs) such as ChatGPT and Gemini for phishing detection and incident response. Whether you're a beginner or a tech enthusiast, this workshop will help you grasp the fundamentals through interactive sessions and hands-on labs. You'll explore how AI can be trained to recognize cyber threats, how machine learning models can be used to classify malicious traffic, and how emerging tools like Secure Multi-Party Computation and Differential Privacy are revolutionizing the way we approach data protection.

## WORKSHOP PREREQUISITES FOR PARTICIPANTS (if any):

• A basic understanding of cybersecurity, including common threats like phishing and malware, as well as concepts like firewalls, encryption, and authentication, will be helpful.

• Additionally, familiarity with AI fundamentals, such as supervised and unsupervised learning, datasets, and neural networks, is beneficial but not mandatory.

• Don't worry if you're new to these topics—we'll cover the essentials during the workshop!.

## SESSION-WISE DESCRIPTION:

**Session 1:**

**Session Time:** 9.30AM - 12.30PM

**Session Topic:** Cybersecurity and Cyber Defense

**Session Description:**
The morning session will lay the groundwork for understanding cybersecurity and its critical role in today's digital landscape. Participants will spend the first 1.5 hours learning about various threats, vulnerabilities, and challenges faced by organizations in the ever-evolving cybersecurity domain. This will be followed by a detailed introduction to cyber defense and cyber threat intelligence (CTI), exploring proactive mechanisms for detecting and mitigating threats while leveraging intelligence for robust defense strategies. The session will conclude with a 30-minute hands-on exercise where participants will implement basic defense setups and experience real-world threat mitigation techniques

**Session 2:**

**Session Time:** 1.30PM - 4.30PM

**Session Topic:** AI/ML in Cybersecurity with Practical PPML Systems

**Session Description:**
The afternoon session will introduce participants to the integration of AI/ML into cybersecurity, focusing on Privacy-Preserving Machine Learning (PPML) and Federated Learning (FL). During the first 1.5 hours, participants will explore these concepts in depth, understanding their methodologies and practical applications in safeguarding sensitive data and enhancing security. The second half of the session will be fully hands-on, allowing participants to engage in real-time testing of a Federated PPML system tailored for cybersecurity scenarios. This interactive segment will provide valuable insights into the performance and practical implementation of these advanced systems.

## Signature of the Secretary

## Signature of the Faculty Advisor