36-Hour Hackathon

Organized by: Hackup Technology Pvt. Ltd.
Date & Time: Starts at **Feb – 12th 9:00 AM (Day-1)** – Ends at **Feb – 13th 9:00 PM (Day-2)**
Venue: K S Rangasamy College of Technology
Participants: UG / PG students interested in **AI, ML, Data Science & Cybersecurity**

Objectives

- Foster innovation in AI, ML, Data Science & Cyber Security.
- Provide hands-on exposure to real-time problem statements.
- Encourage teamwork, design thinking, and rapid prototyping.
- Bridge the gap between academic learning and industry skills.
- Reward outstanding talent with certifications, internships.

Schedule at a Glance

Time	Activity
Day-1	
9:00 – 10:00 AM	**Orientation** • Intro to Hackathon & rules • Demo of pre-vulnerable platforms (HackTheBox, TryHackMe, PortSwigger, VulnHub)
10:00 – 11:00 AM	Team formation & brainstorming
11:00 AM	Hackathon begins
1:00 PM – 02:00 PM	Lunch Break
04:00 PM – 05:00 PM	First Review & mentor feedback (Evaluation-1)
07:00 PM – 08:00PM	Dinner Break
12:00 AM – 1:30 AM	**Ice-breaking session:** IoT Hacking + discussion on recent cyber issues
Day-2	
07:00 – 08:00 AM	Second Review & mentor feedback (Evaluation-2)
01:00 – 02:00 PM	Lunch Break
3:00 – 4:00 PM	Third Review & fine-tuning (Evaluation-3)

07:00 PM – 09:00PM	Final execution & presentations (Final Review – Evaluation-4)
09:00 PM	Valedictory & Awards • CEH voucher announcement • Internship & placement offer for winners

Problem Statements

Teams can select **one** problem to solve.

Core Themes: AI • ML • Data Science • Cybersecurity

1.Automatic Pen-Testing Tool (ML Based)

- **Goal:** Build a server–client tool where the server runs an ML model to detect vulnerabilities on client machines and auto-generate a security report.
- **Impact:** Automates manual pen-testing, helps small organizations secure infrastructure faster.

2.AI Camera for Expression Analysis

- **Goal:** Create a surveillance solution to detect unusual human expressions or gestures and raise early alerts to prevent crimes.
- **Impact:** Assists law enforcement & smart cities in ensuring safety in public areas.

3.Web URL Vulnerability Scanner

- **Goal:** A portal to scan website URLs, detect security flaws (SQLi, XSS, etc.), and generate a professional report.
- **Impact:** Improves website hygiene for SMBs and developers.

4.Mobile App for Cyberbullying Detection & Prevention

- **Goal:** AI-driven mobile application to monitor chats/posts and flag harmful or abusive content.
- **Impact:** Protects students and teens from online harassment.

5. LLM for Cyber Issue SOPs

- **Goal:** Train/Integrate an LLM to answer FAQs and provide SOPs for common cyber issues (content removal, fake profiles, abuse reporting, etc.).
- **Impact:** Empowers the public with instant guidance on handling cybercrimes.

6.SOS & Geo-Fencing App for Women & Elderly

- **Goal:** Mobile app with live location tracking, geo-fencing, and quick SOS alerts to guardians.
- **Impact:** Enhances personal safety in emergencies.

7.LLM Assistant for Forensic Investigators

- **Goal:** Build a model to answer investigators' queries about hardware, USBs, cameras, or system analysis.
- **Impact:** Reduces turnaround time in cyber-forensics.

8.Dark Web Investigation Toolkit

- **Goal:** A dashboard to search, monitor, and analyze suspicious content on the dark web.
- **Impact:** Helps organizations detect stolen credentials and illegal activity.

9.OSINT Framework Portal

- **Goal:** A website that uses free APIs to fetch public data based on name, phone number, email, or social media handle.

- **Impact:** Supports ethical investigators and HR in validating identities.

10.AI-Powered Email Fraud Detector

- Detect phishing and business email compromise attacks using ML algorithms.

11.Ransomware Early-Warning Model

- Build a model to analyze system activity and alert users about potential ransomware behavior.

12.AI Chatbot for Privacy Awareness

- A chatbot to educate users on data privacy, cookies, and safe browsing practices.

13.Insider Threat Detection using ML

- Monitor logins and system usage to identify insider risks in organizations.

14.AI-Based Deepfake Detector

- Detect manipulated videos/images and warn users before sharing.

15.IoT Device Security Analyzer

- A tool to discover IoT devices on a network and assess their vulnerabilities.

Incentives & Recognition

- **Winning Team:** Provided internship by Hackup Technology for Best two performers.
- Certificates for winners and participants.

Target Audience

- UG / PG students in **CSE, IT, AI, ML, Cybersecurity, Data Science**
- Budding ethical hackers, data scientists, and developers.

Requirements for Participants

- Laptops with required IDEs, Python/R, Node.js, OpenCV, scikit-learn, etc.
- Stable internet connection.
- Basic familiarity with coding, AI/ML, or cybersecurity.

Deliverables

- Working prototype / POC of the chosen problem.
- Presentation with use case, solution architecture, and future scope.

Judging Criteria

Criteria	Weight
Problem Understanding	20%
Innovation & Creativity	20%
Technical Implementation	30%
Presentation & Documentation	15%
Feasibility & Impact	15%