Hackathon Guidelines

1. This Hackathon is open to all students from colleges within Tamil Nadu.
2. All topics are applicable to both engineering and arts & science students.
3. Experienced candidates may also apply based on the following criteria:
    - **Topic 1 – Generative AI**:
        i. Candidates with relevant experience of **up to 3 years**.
        ii. Team participation is allowed with a maximum of 3 members per team.
    - **Topic 2 – IoT**:
        i. Candidates with relevant experience of **up to 3 years**.
        ii. Team participation is allowed with a maximum of 3 members per team.
    - **Topic 3 – Cyber Security**:
        i. Candidates with relevant experience of **up to 3 years**.
        ii. Only individual participation is permitted.
    - **Topic 4 – Enterprise Technologies**:
        i. Candidates with relevant experience of **up to 5 years**.
        ii. Only individual participation is permitted.
4. Interested students and candidates must register on the designated portal (**REGISTER NOW**) by submitting their details on or before **19-Jan-2025**.
5. Shortlisted registered participants will be required to submit a presentation of their selected use case between **20-Jan-2025** and **24-Jan-2025**. (Allowed format to be PPT, PDF, doc)
6. The presentations will undergo further evaluation, and the final list of candidates will be announced via email on or before **01-Feb-2025**.
7. The final Hackathon will take place at the **OASYS Institute of Technology** campus.
8. Event dates are **07th February**, **08th February**, and **09th February 2025**.
9. From each topic, the **three best-performing participants** will be selected and awarded prizes along with certificates of excellence.
10. For other selected participants, **HR discussions** will be initiated, and **offer letters or internship** opportunities..
11. Participants must arrange their own travel and accommodation.
12. Food and refreshments will be provided by **OASYS Cybernetics Pvt. Ltd.** during the event.
13. All finalists will receive a **Certificate of Participation** and a memento.
14. Selected candidates must carry an **email confirmation** (soft or hard copy) for verification.
15. Carrying a valid **photo ID proof** (soft or hard copy) is mandatory for participation.
16. Demonstration assets (Hardware, Software) required for the event will be provided by **OASYS Cybernetics Pvt. Ltd.**
17. All submissions must be original and created exclusively during the hackathon. Any form of plagiarism will lead to immediate disqualification.
18. Participants' personal data provided during registration (e.g., name, email, college/company details) will only be used for hackathon-related purposes.
19. Participants must adhere to all guidelines, deadlines, and instructions provided by the Hackathon Committee.

20. For queries, participants can contact via email at **hackathon@oasys.co** or through the provided contact number.
21. The **final decision** on winners and HR considerations lies with the committee.

We look forward to your enthusiastic participation and wish you the best in showcasing your skills!

OASYS Cybernetics Pvt Ltd. – Hackathon-2025 – Use Cases / Problem Statements

Topic 1 – Gen AI

Ref. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
101	HealthCare	**Generative AI solution for healthcare** Build a generative AI solution that solves one or more healthcare problems like building a generative AI chatbot that: Accepts symptom descriptions in natural language and provides likely diagnoses and medical advice (not a replacement for professional consultation). Schedules doctor appointments based on user preferences (time, location, specialization).	A chatbot capable of understanding user queries and providing accurate responses. Integration with an appointment scheduling system or a simulated API. Prototype: A working chatbot or solution that solves a healthcare problem. Code Repository: GitHub repo with proper documentation. Demo Video: 3–5 minutes showcasing the bot/solution in action. Pitch Deck: Description of the problem, solution, architecture, and AI usage.	AI Development: OpenAI GPT-4, Azure OpenAI, or Hugging Face Transformers. Using Open Source LLM like LLAMA-3, Mistral (added advantage). Speech/Text Input: Twilio (for SMS), Dialogflow (for voice), Microsoft Bot Framework, or any open source bot framework. Integration: Google Calendar API, Microsoft Bookings, or a mock scheduling API. Database: Firebase, MongoDB, or SQLite for storing user inputs and preferences. Frontend: React, Angular, or Flutter for building the chatbot interface.
102	Education	**Create a generative AI tutor that:** Explains concepts in a conversational manner. Provides quizzes and interactive exercises. Tailors learning paths based on the student's progress and preferences. Personalized AI Tutor	An engaging educational assistant that adapts to different learning speeds and styles. Integration with a knowledge base of educational content. Prototype: Working AI tutor with a personalized learning path and interactive content. User Journey Map: Showcasing how a student interacts with the platform. Code Repository: GitHub repo with proper documentation.	AI Development: OpenAI GPT-4 or Cohere for generative AI responses. Using Open Source LLM like LLAMA-3, Mistral (added advantage). Content: Khan Academy API or any open-source educational datasets. Frontend: React.js for a web app or native/hybrid mobile apps. Analytics: Google Analytics or Mixpanel for tracking student progress.

Ref. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
			Demo Video: 3–5 minutes showcasing the solution in action. Pitch Deck: Description of the problem, solution, architecture, and AI usage.	Interactive Features: Plotly or D3.js for visualizing quiz results.
103	Accessibility	**AI Document Reader for Visually Impaired Users** Develop an AI assistant that: Converts images of text (e.g., scanned documents, restaurant menus) into speech. Summarizes long documents for quick comprehension. Supports voice-based navigation and customization (e.g., text size, playback speed).	A mobile or web app that provides seamless text-to-speech capabilities and summarization. Ability to recognize and handle multiple languages. Prototype: App capable of extracting text and converting it to speech. Documentation: User manual for accessibility features. Pitch Deck: Explain the impact and scalability of the solution.	OCR: Tesseract OCR or Azure Computer Vision for text extraction from images. Text-to-Speech: Google Text-to-Speech, AWS Polly, Azure Speech Services, or any other free-tier speech services. Frontend: Flutter for cross-platform compatibility or any Native/Hybrid frameworks. Database: Firebase, MongoDB or SQLite for storing recent scans and preferences. Voice Commands: Vosk or Azure Bot Framework with voice integration.
104	Open	You can choose to build a generative AI solution for any problem, that showcases value by impact in improving accessibility, sustainability or value in solving a business problem in any domain like banking and finance, healthcare, telecom, etc Solve a chosen problem in any domain clearly showcasing value	A generative AI solution to any chosen problem. Prototype: Working generative solution for the chosen problem Code Repository: GitHub repo with proper documentation. Demo Video: 3–5 minutes showcasing the solution in action. Pitch Deck: Description of the problem, solution, architecture, and AI usage.	Any available generative AI tool

Topic 2 – IOT

Sl. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
201	Healthcare	**Smart Hospital Management**	- Real-time monitoring of hospital environmental parameters (temperature, humidity, air quality).	- IoT sensors (temperature, humidity, air quality).

Sl. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
		Environmental Monitoring: Design IoT systems that monitor hospital environments for parameters like temperature, humidity, air quality, and infection risks, ensuring a safe and hygienic environment for both patients and staff.	- Automated alerts for anomalies. - Reports on environmental trends.	- Cloud platform for data storage and processing. - Mobile/Web Dashboard.
202	Healthcare	**Elderly Care and Fall Detection** Fall Detection Systems: Design an IoT-powered wearable or home system that detects falls in elderly patients and sends automatic alerts to caregivers, family members, or emergency services.	- Wearable devices or smart home systems for continuous monitoring. - Immediate alerts to caregivers or family during falls. - Data logging for health records and trend analysis.	- IoT-enabled wearables (accelerometers, gyroscopes). - Cloud-based alert system. - Mobile app for caregivers. - ML-based fall detection algorithms.
203	Healthcare	**Healthcare Decision Support System** Clinical Decision Support Systems: Develop a system that integrates real-time IoT data from patients with hospital records and other medical data to support doctors in making more accurate and timely decisions.	- Real-time dashboard integrating IoT data, EHR, and medical records. - Advanced recommendations for clinical decision-making. - Automated alerts for critical parameters.	- IoT devices for patient monitoring. - EHR integration software. - AI decision support systems. - Cloud infrastructure. - Web-based dashboard.
204	Agriculture and Farming	Smart Irrigation Systems: Develop a system that uses soil moisture sensors and weather forecasts to control irrigation systems automatically, conserving water and improving crop yields.	- Automated irrigation controls based on real-time soil moisture and weather data. - Water conservation through precision irrigation. - Alerts for extreme weather conditions.	- Soil moisture sensors. - Microcontrollers (e.g., Arduino, Raspberry Pi). - Weather API integration. - Automated irrigation hardware. - Mobile/Web App.
205	Agriculture and Farming	Livestock Monitoring: Create an IoT solution that tracks the health and activity of livestock using wearable sensors to monitor vitals, movement, and feeding patterns.	- Real-time health and activity tracking for livestock. - Alerts for abnormal vitals or inactivity. - Enhanced livestock health management through data-driven insights.	- Wearable IoT devices (temperature, movement sensors). - GPS trackers. - Cloud platform for data storage. - Mobile App.
206	Agriculture and Farming	Precision Farming: Use IoT-enabled drones and sensors to monitor crops, assess soil health, and make farming practices more efficient.	- Real-time crop monitoring using drones. - Soil health assessment through sensors. - Increased efficiency and reduced resource wastage in farming practices.	- Drones equipped with cameras and sensors. - Soil sensors. - GPS modules.

Sl. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
				- Data analytics tools. - Mobile/Web App.
207	Disaster Management	Flood Monitoring System: Create an IoT-based system using sensors placed in rivers, lakes, or dams to monitor water levels and predict floods in real-time.	- Early flood detection through continuous water level monitoring. - Automated alerts to authorities and communities. - Data analysis for flood risk predictions.	- IoT water level sensors. - GSM/LoRa communication modules. - Cloud platform. - Mobile App for real-time alerts.
208	Retail and Supply Chain Management	Smart Inventory Management: Develop an IoT system that uses RFID or other tracking technologies to monitor stock levels in real-time, sending alerts when items are low and optimizing restocking.	- Real-time stock tracking using RFID and IoT. - Automated restocking alerts. - Optimization of inventory levels and reduction in stockouts.	- RFID tags and readers. - IoT-enabled shelves. - Cloud platform for data storage. - Inventory management software.
209	Retail and Supply Chain Management	Supply Chain Transparency: Create an IoT solution that tracks products from production to delivery, providing transparency and ensuring the integrity of the supply chain.	- End-to-end supply chain visibility. - Real-time tracking of product location and condition. - Improved customer trust through transparent supply chain practices.	- IoT trackers. - GPS modules. - QR based Track and Trace - Cloud platform. - Supply chain monitoring softwa

Topic 3 – Cyber Security

Sl. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
301	Network Forensics & Incident Response	An organization has been compromised by a malicious malware attack after a user inadvertently clicked on a malicious document, triggering the malware to execute and propagate across the network. As a cybersecurity analyst, your task is to perform a comprehensive incident analysis and root cause investigation using the provided Packet Capture (PCAP) file. You must identify	Perform detailed incident analysis and root cause investigation using the provided Packet Capture (PCAP) file, and deliver an incident analysis report that should include the following: Detailed sequence of events: Infection, malware execution, propagation, C&C communication. Identification of affected systems: IP addresses, hostnames, and behaviors. Indicators of Compromise (IOCs): IPs, domains, file	- Packet analysis software tools - IOC visualization & Correlation - Mapping out attack infrastructure and threat actor networks through the softwares - Network protocol analyzer

Sl. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
		suspicious traffic, pinpoint affected systems, extract Indicators of Compromise (IOCs), trace the malware's movement, and determine the attack's origin. Based on your findings, you are expected to deliver a detailed incident report, including a timeline of the attack, a list of compromised systems, IOCs, and remediation steps to contain the incident and prevent future breaches	hashes, URLs, ports, protocols, email addresses. Root Cause Analysis: Identify the initial infection vector (e.g., phishing), malware type, and behavior. Future Prevention & Remediation steps: Recommended actions to prevent future attacks and steps to remediate the current incident.	
302	Web Application Exploitation	Your task is to find a secret flag intentionally hidden within a vulnerable web application. The application is hosted inside a Docker machine, and you are required to set up and deploy the Docker machine locally to run the web application. Once the environment is set up, you must perform a series of attacks, exploiting a chain of vulnerabilities in the application to locate and capture the hidden flag. As you conduct the attack, you are expected to identify and document each vulnerability separately, detailing the steps taken to exploit them and how they contributed to progressing through the attack chain. Finally, you must deliver a comprehensive report, including a step-by-step breakdown of the vulnerabilities identified, how they were chained together, and a clear explanation of how you successfully found the hidden flag within the application.	Vulnerability Identification: Document each vulnerability discovered within the application. Exploitation Steps: Detail the steps taken to exploit each vulnerability. Vulnerability Chain Analysis: Explain how each vulnerability contributed to progressing through the attack chain. Flag Discovery: Describe how the vulnerabilities led you to find the hidden flag within the application. Comprehensive Report: Provide a step-by-step breakdown of the identified vulnerabilities, exploitation methods, and the process of capturing the flag.	- Vulnerability exploitation & analysis tools. - Docker environment setup - Virtualization Software (Optional) - Intercepting proxy tools for the web traffic analysis & exploitation. - Command line & custom scripts, tools
303	Cryptographic Analysis	Your task is to perform a cryptographic analysis on a given encrypted file to		- Cryptographic Libraries & Tools - Command line & custom scripts & tools

Sl. No.	Domain	Problem Statement / Challenges	Expected Outcome / Deliverables	Hardware / Software
		enumerate the private key and decode the cipher to reveal the internal secret flag. The file contains encrypted data, and you must apply your knowledge of cryptographic algorithms and techniques to break the encryption. You will need to analyze the file's structure, identify the cryptographic methods used, and extract any necessary keys or parameters. Once the private key is enumerated, you should use it to decrypt the cipher and uncover the hidden flag. Finally, you are expected to deliver a detailed report explaining the cryptographic techniques applied, the steps taken to extract the private key, and all the process & steps used to successfully decrypt the file and retrieve the secret flag.	A Detailed Report with step-by-step breakdown of the cryptographic techniques applied, method used to extract the private key and decryption process used to successfully retrieve the secret flag & tools used for it along with POC's Cryptographic Analysis: Analyze the encrypted file to determine its structure and identify the cryptographic algorithm used (e.g., RSA, AES, ECC, etc.). Key Enumeration: Extract the necessary keys or parameters (e.g., private key, encryption key, or decryption parameters). Decryption Process: Use the identified cryptographic techniques and private key to decrypt the cipher and reveal the hidden flag.	- Hex editors - Decryption software tools

Topic 4 – {Enterprise Technologies}

Ref. No.	Domain	Tech Stack
401	Backend Developer	Java with Spring Boot/Node JS/Python, Kafka/RabbitMQ, Hibernate
402	Front End Developer	Angular/React
403	FullStack Developer	Java with Spring Boot/Node JS/Python, Kafka/RabbitMQ, Hibernate
		Angular/React
404	DataBase Administrators	SQL/NOSQL/GRAPHQL
405	Mobile App Development	Android/IOS Native, Hybrid Frameworks
406	Big Data	Big data technologies