



CRYPTAURA 2.0

PROBLEM STATEMENTS

S. No.	Problem Statement ID	Theme	Problem Statement Title	Problem Description	Expected Solution
1	AURA-1.1	Network & Infrastructure Security	Detecting Automated Attacks on Indian Digital Services	Indian websites, APIs, and digital services face automated attacks such as credential stuffing, bot traffic, scanning, and brute-force attempts.	Build a lightweight system that identifies abnormal and automated network behaviour from simulated traffic and distinguishes legitimate users from malicious bots.
2	AURA-1.2	Network & Infrastructure Security	Low-Cost Cyber Defence for Educational Institutions	Many schools, colleges, and small institutions operate with limited cybersecurity budgets and technical staff, making them attractive targets for attacks.	Develop an affordable network-security solution capable of detecting suspicious traffic, unauthorized access, and common attacks without requiring an enterprise SOC.
3	AURA-2.1	Application Security	Securing APIs for Digital India Services	Modern Indian applications depend heavily on APIs for payments, e-commerce, education, healthcare, and government platforms. Poorly protected APIs can	Build an API security layer that detects authentication weaknesses, injection attempts, excessive requests, and unauthorized API access.



Vel Tech Multi Tech

Dr.Rangarajan Dr.Sakunthala Engineering College

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai)

				expose sensitive information.	
4	AURA-2.2	Application Security	Preventing Unauthorized Access to User Data	An application may correctly authenticate a user but still allow them to access another user's information by manipulating IDs or API requests.	Develop a tool that automatically tests a simulated application/API for broken object-level authorization and identifies where users can access resources they do not own.
5	AURA-3.1	Cryptography & Data Protection	Protecting Sensitive Indian Digital Data	Organizations handle sensitive information such as identity details, financial records, academic information, and customer data. Poor encryption and key management can lead to serious data exposure.	Build a secure system for encrypting sensitive data, managing cryptographic keys, rotating keys, and revoking compromised keys.
6	AURA-3.2	Cryptography & Data Protection	Detecting Exposed Secrets in Applications	Developers frequently accidentally expose API keys, database passwords, tokens, and other credentials through source code, Git repositories, or configuration files.	Build a tool that scans source code and project files for hardcoded secrets and weak cryptographic practices.
7	AURA-4.1	Digital Forensics & Incident Response	Reconstructing a Ransomware Attack	Indian educational institutions, businesses, and organizations can lose access to critical systems during ransomware incidents. Investigators need to understand how the attack occurred.	Given simulated logs from a ransomware incident, reconstruct the attack from initial access → privilege escalation → lateral movement → encryption → data theft.



Vel Tech Multi Tech

Dr.Rangarajan Dr.Sakunthala Engineering College

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai)

8	AURA-4.2	Digital Forensics & Incident Response	Investigating Digital Payment Fraud	UPI and other digital payment systems have created new opportunities for fraud involving phishing, fake payment requests, account takeover, and social engineering.	Analyze a simulated dataset containing transaction records, device information, login events, and communication logs to identify how a fraudulent transaction occurred.
9	AURA-5.1	IoT & Embedded Security	Securing Smart Healthcare Devices	Hospitals increasingly use connected devices such as patient monitors, smart sensors, and networked medical equipment. A compromised device could affect both data and operations.	Build a monitoring system that detects abnormal behaviour from a simulated healthcare IoT environment.
10	AURA-5.2	IoT & Embedded Security	Securing Smart Homes & Connected Devices	Smart cameras, routers, locks, sensors, and other IoT devices are becoming common in Indian homes, but many users do not understand their security risks.	Develop a tool that identifies insecure configurations, weak credentials, unusual device behaviour, and unauthorized communication within a simulated smart-home network.
11	AURA-6.1	Cloud Security	Cloud Security for Indian Startups & MSMEs	Startups and MSMEs increasingly depend on cloud platforms but may lack dedicated cloud-security teams. Misconfigured storage, databases, and access controls can expose sensitive information.	Build a tool that scans a simulated cloud environment and identifies insecure configurations such as public storage, exposed services, and excessive permissions.



Vel Tech Multi Tech

Dr.Rangarajan Dr.Sakunthala Engineering College

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai)

12	AURA-6.2	Cloud Security	Detecting Excessive Cloud Permissions	Compromised credentials can give attackers access to far more resources than they actually need.	Analyze a simulated cloud IAM environment and identify over-privileged users, unused accounts, risky roles, and privilege-escalation paths.
13	AURA-7.1	AI/ML for Cybersecurity	Detecting AI-Generated Scams & Phishing	Generative AI allows scammers to create convincing phishing emails, SMS, and social-media messages in multiple Indian languages.	Build an AI system that detects suspicious messages and distinguishes between legitimate communication, traditional phishing, and AI-generated scams.
14	AURA-7.2	AI/ML for Cybersecurity	Securing AI Chatbots from Prompt Injection	AI chatbots used by organizations can be manipulated through malicious prompts to reveal confidential information or perform unauthorized actions.	Build a security layer that identifies and prevents prompt injection, sensitive-data leakage, and unauthorized tool usage in a simulated AI application.
15	AURA-8.1	Social Engineering & Human Factor	UPI & Digital Payment Scam Detection	Many digital-payment scams rely on social engineering rather than technical exploitation. Attackers may impersonate bank officials, customer-care agents, delivery companies, or known contacts.	Develop a system that analyzes simulated SMS, WhatsApp messages, emails, QR/payment requests, and phone-call transcripts to identify potential scams.
16	AURA-8.2	Social Engineering & Human Factor	Deepfake Impersonation Protection	AI-generated voice and video can be used to impersonate family members, company executives, public officials, or	Build a system that analyzes simulated audio/video communications and identifies indicators of



Vel Tech Multi Tech

Dr.Rangarajan Dr.Sakunthala Engineering College

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai)

				financial representatives.	AI-generated or manipulated content.
17	AURA-9.1	Intelligent Industry & Manufacturing	Detecting Hidden Failure Patterns in Industrial Machines	Industrial machines often produce early warning signals—changes in vibration, temperature, current, pressure, or operating cycles—before a failure occurs. These signals are usually collected independently, making it difficult to identify combinations that indicate an upcoming failure.	Build a system that correlates multiple simulated machine parameters and identifies early-stage failure patterns rather than simply detecting when a parameter crosses a fixed threshold.
18	AURA-9.2	Intelligent Industry & Manufacturing	Optimizing Production Under Machine Constraints	In manufacturing, production schedules must consider machine availability, energy consumption, maintenance windows, processing time, and delivery deadlines.	Develop an optimization engine that generates a production schedule while balancing machine capacity, energy usage, maintenance requirements, and delivery deadlines.
19	AURA-10.1	Energy, Power & Infrastructure Intelligence	Detecting Non-Technical Losses in Electrical Distribution	Electricity distribution systems can experience losses that are not explained by normal technical losses. Detecting suspicious consumption patterns using only individual meter readings can be difficult.	Build an analytics system that analyzes simulated feeder, transformer, and consumer-meter data to identify abnormal consumption patterns and probable loss locations.
20	AURA-10.2	Energy, Power &	Grid-Aware EV Charging Optimization	Large-scale EV charging can create localized peaks in electricity demand.	Develop an intelligent charging scheduler that determines when and how much each



Vel Tech Multi Tech

Dr.Rangarajan Dr.Sakunthala Engineering College

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai)

		Infrastructure Intelligence		Charging every vehicle immediately may not be the optimal strategy for the distribution network.	EV should charge while considering battery requirements, user deadlines, charging-station capacity, and simulated grid load.
21	AURA-11.1	Climate, Water & Resilient Infrastructure	Predicting Urban Water-Pipeline Failures	Water distribution networks contain pipelines operating under different pressures, ages, materials, and environmental conditions. Failures can cause large water losses and service disruption.	Build a system that combines simulated pressure, flow, pipe age, material, maintenance history, and environmental data to identify sections at higher risk of leakage or failure.
22	AURA-11.2	Climate, Water & Resilient Infrastructure	Infrastructure Damage Assessment from Images	Inspecting roads, bridges, and concrete structures manually is time-consuming and may miss early-stage defects.	Develop a computer-vision system capable of detecting and classifying simulated infrastructure defects such as cracks, potholes, surface deterioration, or structural anomalies from images.
23	AURA-12.1	Connected Systems, Robotics & Edge Intelligence	Reliable Communication for Disaster-Response Robots	During disasters, communication infrastructure may become unreliable or unavailable. Robots or field sensors still need to exchange critical information.	Design a communication architecture for simulated rescue robots/sensors that can continue transmitting critical data under intermittent connectivity.
24	AURA-12.2	Connected Systems, Robotics & Edge Intelligence	Multi-Robot Task Allocation in Unknown Environments	When multiple robots are deployed for inspection, search, or disaster response, assigning the nearest robot to	Build an algorithm that dynamically assigns tasks among multiple simulated robots based on distance, battery level, robot



Vel Tech Multi Tech

Dr.Rangarajan Dr.Sakunthala Engineering College

An Autonomous Institution

(Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai)

				every task can cause duplicated work, battery depletion, and communication bottlenecks.	capability, task priority, communication availability, and environment conditions.
25	AURA-13.1	Digital Trust, AI & Human-Centric Engineering	Detecting Manipulated Sensor Data in Critical Systems	Modern industrial, healthcare, energy, and transportation systems depend on sensor data. If sensor readings are manipulated, the control system may make incorrect decisions.	Build a system that identifies physically inconsistent or manipulated sensor readings by correlating multiple sensor streams.
26	AURA-13.2	Digital Trust, AI & Human-Centric Engineering	Trustworthy AI Decision Auditor	AI systems are increasingly used to make decisions from images, sensor data, documents, and user information. A prediction alone is insufficient when engineers need to understand whether the decision can be trusted.	Develop an AI auditing layer that evaluates an AI model's output for confidence, data quality, out-of-distribution inputs, possible bias, explanation of the decision, and potentially unsafe predictions.