PANIMALAR ENGINEERING COLLEGE

An Autonomous Institution

[JAISAKTHI EDUCATIONAL TRUST]

Approved by AICTE | Affiliated to Anna University | Recognized by UGC

All Eligible UG Programs are Accredited by NBA

Bangalore Trunk Road,Varadharajapuram, Poonamallee, Chennai- 600 123

INDIA'S WOMEN CENTRIC NATIONAL LEVEL 24 – HOUR HACKATHON

TECHDIVATHON – 2.0

She blooms. She leads. She conquers

Domain:CYBERSECURITY

Problem Statements:

S.No	Title	Problem Statement	Description
1	AI-Powered Detection System	Deepfake content spreads misinformation and risks reputational harm.	Design a tool that uses AI to analyze media and detect manipulated images, videos, voice recordings in real time, flagging deepfakes for users and platforms.
2	Quantum-Resistant Secure Messaging App	Quantum computers threaten existing encryption protocols.	Develop a secure communications platform that implements post-quantum cryptography, ensuring long-term privacy and resistance to quantum attacks.
3	Cloud Supply Chain Vulnerability Tracker	Cloud-based supply chains are exposed to hidden third-party breaches.	Build a dashboard that maps, monitors, flags vulnerabilities or breaches in cloud vendor ecosystems, alerting organizations to indirect security risks.
4	Insider Threat Prediction Platform	Insider data breaches remain undetected until significant loss occurs.	Create an AI system that analyzes user behavior to proactively predict and alert on potential insider threats within organizations.
5	Autonomous Ransomware Isolation Gateways	Ransomware often spreads laterally before detection.	Design a network gateway that autonomously identifies, classifies, and isolates ransomware traffic before it can spread to other systems.
6	IoT Device Firmware Integrity Scanner	IoT device firmware updates are a major point of vulnerability.	Build a platform to remotely scan, verify, and validate the authenticity and integrity of firmware running on enterprise and consumer IoT devices.
7	AI-Driven Social Engineering Trap Platform	Advanced phishing and social engineering tactics exploit employees' trust.	Develop a platform that simulates social engineering attacks, learns user weaknesses, and provides adaptive, gamified training to increase awareness.
8	AI-Augmented Browser Anti-Phishing Extension	Traditional phishing detection struggles with dynamic scam sites.	Create a browser extension that leverages AI to analyze page structure and behavior in real time, warning users of suspicious or new phishing sites.

9	Privacy-Preserving Biometric Authentication	Users worry about biometric data theft and misuse.	Invent a system that performs secure, privacy-preserving biometrics—e.g. zero-knowledge proofs for face or fingerprint access—without storing raw data.
10	Distributed Denial-of-Service Early Warning Sensor	DDoS attacks overwhelm platforms with little warning.	Design a distributed sensor network that monitors key Internet infrastructure for DDoS precursors, alerting affected networks early to mitigate attacks.
11	AI-Driven Industrial Threat Detector	Industrial networks (ICS/OT) lack timely threat visibility.	Develop an AI-driven sensor suite that learns normal traffic/behavior patterns and instantly flags anomalous, potentially malicious control activity
12	Secure Multi-Party Computation Suite	Organizations need to jointly analyze data without sharing sensitive information.	Build a toolkit enabling parties to run computations on shared, encrypted datasets with zero data exposure, applicable for finance, law, and research.
13	Smart Hospital Electronic Health Record Guardian	Healthcare EHRs face targeted data theft.	Create a smart guardian that continuously monitors access/logs to EHR systems, flags anomalies, and auto-locks sessions showing adversarial behavior.
14	False News and Disinformation Filter	Disinformation campaigns harm public trust in media and democracy.	Invent a tool that uses AI and network analysis to detect, flag, and filter coordinated false information campaigns on social platforms.
15	Remote Access & Cheating Detection	Online exams on unmanaged third-party devices are vulnerable to remote access, screen sharing, AI assistance, and virtual machines.	Build a mechanism using behavioral analysis, process monitoring, network traffic inspection, and AI anomaly detection to identify and prevent cheating attempts including remote desktop access, screen sharing tools, unauthorized VMs, and real-time AI assistance during exams.
16	Blockchain Smart Contract Auditor	Bugs in smart contracts lead to huge crypto thefts and exploits.	Build an automated engine to scan, simulate, and validate blockchain smart contracts for known and unknown vulnerabilities before deployment.
17	Secure Candidate Authentication on Untrusted Devices	Online CBT systems running on third-party infrastructure risk impersonation and identity fraud due to lack of hardware/OS control.	Develop a zero-trust authentication platform using multi-factor biometrics (face, voice, behavioral), hardware-bound cryptographic attestations, and remote proctoring AI that ensures candidate identity verification and prevents proxy test-taking on untrusted devices.
18	Autonomous Public Wi-Fi Threat Scanner	Open networks are exploited for attacks and data interception.	Create a portable device or app that scans public Wi-Fi areas for intercept risks, ARP spoofing, and suspicious endpoints, notifying users instantly.
19	AI-Driven Fraudulent Transaction Alert Platform	Payment fraud is outpacing manual oversight and static rules.	Build an AI-powered financial monitoring service that detects and halts real-time fraudulent transactions across banks and e-commerce.
20	End-to-End Secure Digital Signature Platform	Document tampering threatens contract authenticity.	Develop a secure e-signature solution leveraging hardware tokens and real-time blockchain notarization to prove the origin and integrity of signed files.

21	Edge AI Threat Analysis for Connected Vehicles	Autonomous vehicles are vulnerable to network attacks.	Invent an edge AI module for cars that inspects inbound/outbound communications, identifies suspicious activity, and enforces safety-critical restrictions.
22	Privacy Dashboard for Smart Homes	Users lack visibility into data flow from connected home devices.	Create a dashboard showing which devices share what data, where it goes, with suggested steps to limit exposure, driven by real-time alerts.
23	AI-Driven Credential Theft Honeytoken Suite	Stolen credentials often go undetected until after breach.	Develop honeytoken credentials—unique decoys monitored by AI—that instantly alert defenders to leaks or credential harvesting attempts.
24	Autonomous Firmware Rollback Protection	Firmware supply chain attacks silently brick or backdoor devices.	Engineer a device-agnostic system that verifies signed firmware, detects malicious updates, and auto-rolls back to last-known-safe versions.
25	Zero-Trust Online Examination Framework	Online CBT platforms lack continuous validation of identity, device, and session integrity on untrusted infrastructure.	Create a zero-trust CBT framework that continuously validates candidate identity, device integrity, and session authenticity using multi-layered biometrics, cryptographic attestations, behavioral analysis, and real-time anomaly detection, assuming every component is untrusted

Reviewer's Digital Signature

Reviewer's Name:
Position:
Organization:
Date:

Digital Signature: