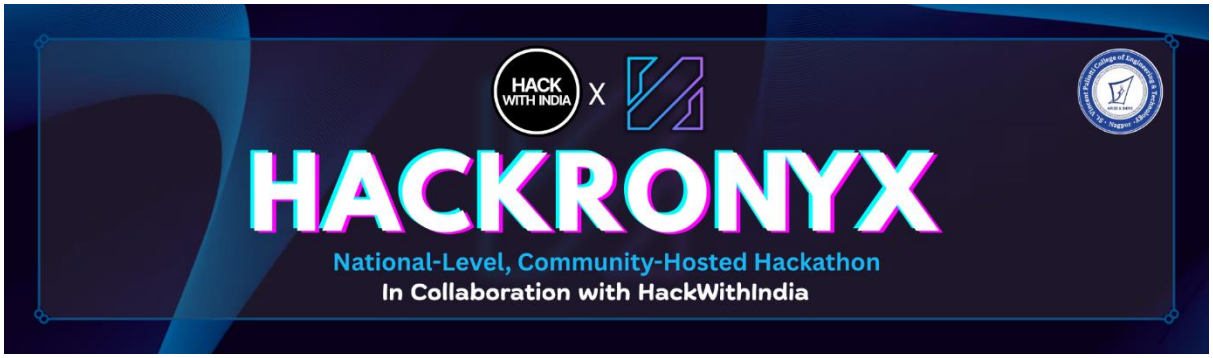

ROUND 1 - PROBLEM STATEMENTS

Participants are encouraged to leverage any technology—whether it's artificial intelligence, blockchain, cybersecurity, data analytics, or others—to develop their solutions. There are no restrictions on the tools or platforms used, as long as the approach is innovative, addresses the core problem effectively, and demonstrates practical feasibility for real-world implementation.

PPT GUIDELINES:

Submit the PPT in PDF Format.

Page 1: Introduction

Page 2: Problem overview (Mention PS ID)

Page 3: Solution overview

Page 4: Technical deep dive

Page 5: Implementation details

Page 6: Feasibility analysis

Page 7: Team members (Also mention LinkedIN Id's)

PS ID	Title	Description
R1-01	Inventory Misalignment in Multi-Warehouse Logistics	A national logistics company operating multiple warehouses across regions often experiences inventory discrepancies, leading to overstock in some locations and stockouts in others. Despite using ERP systems, issues persist due to inaccurate demand forecasting, inefficient inter-warehouse transfer coordination, and a lack of real-time visibility. How can this imbalance be addressed while keeping operational costs low?

R1-02	Unplanned Downtime in Mid-Sized Manufacturing Units	Manufacturing SMEs often suffer unplanned machine downtime, leading to production delays and increased maintenance costs. These units usually lack advanced monitoring systems and operate with minimal digital infrastructure. What kind of system or process can help these facilities anticipate failures and schedule maintenance proactively?
R1-03	Digital Trust Without Digital Clutter	Online users frequently share personal data across apps, sites, and services without knowing how it's stored, shared, or used. Most don't read privacy policies or understand consent frameworks. Meanwhile, developers build authentication systems, yet ignore transparency or user control. Developers focus on login systems but overlook transparency and user autonomy. What kind of solution can empower users to take control of their digital identity and data relationships, while being easy for developers to integrate? You might build a digital-passport, or an extension, or a dashboard, or maybe a plug-and-play API! The innovation is yours…
R1-04	Trust Gaps in Supply Chain Traceability	In global supply chains—especially for products like pharmaceuticals, luxury goods, or perishables—tracking the origin and movement of goods is difficult, often relying on siloed, error-prone records. This creates vulnerabilities to fraud, counterfeiting, and regulatory non-compliance. There's a growing demand for systems that offer traceability, integrity, and transparency across multiple parties without relying on centralized control. Participants can explore solutions for ledger system, authenticity, or even sharing layer!
R1-05	Enhancing Job Screening	The recruitment process often involves manually reviewing numerous job descriptions (JDs) and CVs, which can be time-consuming and prone to human error. The goal of this hackathon is to develop a multi-agentic Al system that can automatically read and summarize job descriptions (JDs), match candidate qualifications with the JD, shortlist candidates, and send interview requests based on the match. Participants are expected to make a multiagent framework.

R1-06	Defending National Web Infrastructure from Targeted Attacks	Government websites, financial portals, and public service platforms are frequently targeted by coordinated cyberattacks such as DDoS, defacement, or data exfiltration—especially during geopolitical tensions. These attacks can disrupt critical services, erode public trust, and compromise sensitive data. Many institutions still rely on outdated security infrastructure and lack proactive detection or rapid mitigation capabilities. Participants are challenged to build solutions that detect and block unusual traffic patterns, trace the origin of suspicious requests without violating privacy, or create real-time dashboards for monitoring and responding to infrastructure-level threats. The solution should be lightweight, scalable, and adaptable to different types of public-facing web applications.