Hackathon Problem Statement:

"Real-Time Fraud Prevention: Building AI-Powered Call Scam Detection for Safer Communication"

Objective:

Develop an innovative solution to protect users, particularly vulnerable groups such as elderly individuals, from falling victim to scam or fraudulent phone calls by leveraging AI-powered real-time audio analysis and fraud detection.

Problem Context:

With the rise of digital fraud and phone scams, many individuals are at risk of losing sensitive information, money, or personal security. Vulnerable groups, such as the elderly, are particularly targeted. Despite existing measures like spam call filters, there is a lack of real-time, conversational safeguards to detect scams during live interactions.

Expected Solution Features:

Participants are tasked with creating a solution that can:

1. **Real-Time Audio Analysis:**
    - Develop a mobile or web application that listens to live phone calls or simulated interactions.
    - Use AI/ML models to analyze the conversation in real time and identify patterns or keywords indicating potential fraud (e.g., requests for OTPs, personal information, or installation of remote access apps).
2. **Risk Alert System:**
    - Provide immediate and clear warnings when suspicious activity is detected.
    - Offer actionable suggestions such as disconnecting the call, asking clarifying questions, or refraining from sharing sensitive information.
3. **Adaptive Learning:**
    - Continuously improve detection accuracy by adapting to new scam patterns or phrases via user feedback or updates to the language model.
4. **Privacy & Security:**
    - Ensure the app processes audio data securely and locally where possible, respecting user privacy and compliance with regulations like GDPR or CCPA.

Challenge Scope:

- Integrate **speech-to-text processing** with a robust **NLP pipeline** for fraud detection.
- Develop or utilize a blacklist of known scam words, phrases, and behavioral indicators.
- Create an intuitive user interface accessible to all demographics, especially elderly users.

- Propose scalable architecture for deploying the solution globally, considering multilingual support.
- Bonus: Include an **educational module** to inform users about common scam tactics and preventive measures.

Example Use Case:

An elderly user receives a call from someone posing as a bank representative. The app listens to the conversation and detects phrases like “confirm your OTP” or “install the AnyDesk app.” It immediately flags the call as high-risk, displays a warning to the user, and suggests they disconnect the call.

Evaluation Criteria:

1. **Innovation:** Novelty and creativity in the solution approach.
2. **Accuracy:** Effectiveness of scam detection algorithms.
3. **User Experience:** Accessibility, simplicity, and clarity of the interface.
4. **Scalability:** Feasibility to adapt the solution for diverse user bases, languages, and use cases.
5. **Privacy & Ethics:** Adherence to data privacy laws and ethical considerations.

We encourage participants to think outside the box and create impactful solutions that can make a real-world difference!