problem statements for the **Cyber Security and Blockchain theme** of KuruKshetra-25 hackathon.

Hackathon Theme 2: Cyber Security and Blockchain

Blockchain Focus Areas

1. Blockchain-Enabled Federated Learning for Privacy-Preserving Collaboration

- **Objective:** Train shared ML models across multiple organizations without sharing raw data.
- **Approach:**
  - Combine **federated learning** with **blockchain** for decentralized trust.
  - Store model updates immutably on a distributed ledger.
  - Use **smart contracts** for secure aggregation (no central coordinator needed).
- **Features:**
  - Apply **differential privacy** to protect sensitive records (e.g., hospital data).
  - Demonstrate accuracy comparable to centralized models.
  - Ensure transparency, tamper-proof updates, and traceability.

---

2. Fair Finance AI on Blockchain (Fraud Detection & Bias-Free Lending)

- **Objective:** Build a transparent financial system for fraud detection and fair credit scoring.
  Approach:
  - Train AI models to detect fraudulent transactions and ensure unbiased loan approvals.
  - Store all **model training data, fairness checks, and decision logs** on blockchain for full transparency.
- **Example:**
  - A credit scoring model approves loans at equal rates for men and women with similar profiles.
  - Regulators can verify fairness using blockchain audit trails.

Cyber Security Problem Statements

Problem 0: Secure ML Pipelines (Data Poisoning Prevention)

- **Objective:** Ensure robustness of machine learning training pipelines against data poisoning or adversarial contamination.

- **Problem:** Attackers can inject malicious data to implant biases or backdoors into models (e.g., LLM training).

- **Goal:**

    - Build safeguards that scan and verify incoming training data (e.g., user-submitted content).

    - Use anomaly detection, provenance checks, or other scalable methods.

- **Challenge:** Achieve strong vetting without compromising training scalability.
- **Reference:** Research indicates data poisoning can undermine ML models (see arxiv.org).

Problem 1: Email Spoofing Detection

- **Goal:** Identify and flag emails with manipulated sender information.
- **Context:**
    - Email spoofing enables phishing, malware delivery, and business email compromise (BEC).
    - Attackers manipulate SMTP headers (`From`, `Reply-To`, `Return-Path`) to impersonate trusted sources.

Problem 2: Phishing Detection Solution

- **Goal:** Design an AI-enabled phishing link detection and alert system.

- **Features:**

    - Detects malicious links on web pages, email apps, messaging platforms, and social media.
    - Deliver as a **desktop/mobile app** or **browser plugin** to warn users in real time.

Problem 3: Layering of Bank Accounts (Money Laundering Detection)

- **Goal:** Visualize suspicious money trails across bank accounts.
- **Features:**
    - Build **spider maps or nodal graphs** to track movement between accounts.
    - Link inter-case bank layers and filter by account holder, IP, phone, email.

- **Expected Result:** Help law enforcement trace source and destination of illicit funds efficiently.

Problem 4: Social Media Record Finder Tool

- **Goal:** Build an open-source platform to link identities across platforms using public data.

- **Functionality:**

    - Input: mobile number or email.
    - Output: linked accounts (Facebook, Instagram, Twitter, Paytm, TrueCaller, UPI, etc.).

- **Use Case:** Assist police investigations through social engineering data aggregation.

Problem 5: VoIP Call Tracing

- **Goal:** Develop advanced techniques to trace internet calls.

- **Features:**
    - Identify IMEI or capture IP details of VoIP callers.
    - Detect and trace virtual numbers generated using rogue apps.
- **Expected Result:** Enable law enforcement to locate internet callers in real time.

Problem 6: Autonomous AI-Based Threat Detection & Elimination

- **Goal:** Build an AI engine to detect and block **ransomware** and **zero-day attacks** in cloud services.
- **Features:**
  - Automated alert management.
  - Analytics to evaluate false positives.
  - Reduced workload for security analysts.

Problem 7: Attack Surface Monitoring Tool

- **Goal:** Continuous discovery, analysis, remediation, and monitoring of vulnerabilities.
- **Future Expectations:**
  1. Fully automated detection and remediation.
  2. Integrity/configuration checking.
  3. Patch management for on-premises and cloud.
  4. Standard APIs for integration.

Problem 8: Securing Document Handling for Non-Tech-Savvy Users

- **Goal:** Design a secure, traceable document-sharing and printing system for low-tech environments (e.g., rural internet cafés).
- **Key Points:** Balance strong security with user-friendliness to prevent data misuse.

Problem 9: AI-Powered Ransomware Detection & Response

- **Features:**
  1. ML-based ransomware behavior detection.
  2. Real-time monitoring of file/system activity.
  3. Automated response and containment.
  4. Forensic reporting for post-attack analysis.

Problem 10: AI-Powered Web Vulnerability Scanner & Auto-Patcher

- **Goal:** Detect and patch vulnerabilities automatically.
- **Features:**
  - AI-enhanced scanning accuracy with low false positives.
  - Severity-rated reports with suggested fixes.
  - Automated patch deployment via an intuitive interface.

Problem 11: AI-Driven Web Application Firewall (WAF)

- **Goal:** Build a WAF with adaptive, ML-generated rules.
- **Features:**
  - Real-time malicious traffic detection.
  - Self-updating rules with minimal false positives.
  - Explainable AI insights for security teams.

Problem 12: Verified Download Link Suggestion Tool

- **Goal:** Help users avoid malicious software download links.
- **Approach:** Create a plugin or app to verify safe download sources before clicking.

Problem 13: Insider Threat Detection System

- **Goal:** Detect malicious or accidental insider risks in organizations.
- **Features:**
    - Continuous user behavior monitoring (UBM).
    - Anomaly detection (e.g., off-hours access, large file transfers).
    - Risk scoring, access trail visualization, and behavioral forensics.

Problem 14: Deepfake Video and Voice Detection

- **Goal:** Develop AI tools to identify synthetic media.
- **Features:**
    - Detects facial inconsistencies, abnormal voice modulation, lip-sync mismatches.
    - Provide authenticity scores and metadata trails.
    - Integration with digital evidence systems for law enforcement.

Problem 15: Geo-Fencing Alert System for Criminal Movements

- **Goal:** Real-time tracking of high-risk individuals via GPS/geofencing.
- **Features:**
  - Alerts when suspects enter restricted zones.
  - Dashboard to monitor multiple individuals.
  - Optional integration with facial recognition from public CCTV.

Problem 16: SIM Swap Detection and Alert System

- **Goal:** Identify and block fraudulent SIM porting attempts.
- **Features:**
  - ML-based detection of unusual SIM or device changes.
  - Integrated alerts in mobile banking apps or email providers.

Problem 17: AI-Based Criminal Profiling and Threat Assessment

- **Goal:** Predict high-risk individuals or zones based on historical data.
- **Features:**
  - Risk scoring from criminal history, social media, financial records.
  - Clear disclaimers, audit trails, and safeguards to prevent bias or misuse.

Problem 18: AI-Powered Screenshot Classifier

- **Goal:** Automate classification of screenshots for investigations.
- **Features:**
  - Categorize chats, transactions, threats, adult content, etc.
  - Multi-language OCR, entity recognition, and tagging.
  - Search, filter, and export options for legal reporting.

Problem 19: Digital Rumor Spread Mapping and Source Detection

- **Goal:** Trace viral rumors or fake news back to originators.
- **Features:**
  - Timeline and geographical spread mapping.
  - Visualization of rumor trees and user clusters.
  - Sentiment analysis and source credibility scoring.

Problem 20: Password Reuse and Breach Exposure Checker

- **Goal:** Protect end-users from using compromised credentials.
- **Features:**
  - Check email/password against breach databases (e.g., Have I Been Pwned).
  - Notify users and suggest strong password replacements.
  - Privacy-preserving browser extension or mobile app.