■ Federated Cyber-Insurance Risk Assessment (Fed-CyRA)

Creating a Trustless, Collaborative Cyber-Risk Model

Fed-CyRA is an innovative **privacy-preserving federated learning framework** designed to transform the cyber-insurance industry. It enables multiple insurers to collaboratively train a powerful breach prediction model — without sharing their clients' sensitive data. By turning competitive confidentiality into a collaborative advantage, Fed-CyRA revolutionizes how cyber-risk is measured, priced, and mitigated.

■ The Problem

- Cyber-insurers operate with isolated data silos, leading to poor generalization and inaccurate risk pricing.
- Premiums often rely on incomplete data, resulting in unfair rates and heavy financial losses.
- New threats and zero-day vulnerabilities evolve rapidly, but insurers lack shared intelligence to respond in time.
- There is no secure or trustless mechanism for collaborative learning among competitors.

■ The Solution: Fed-CyRA

Fed-CyRA proposes a **federated cyber-risk assessment network** allowing insurers to jointly train a breach prediction model. Each participant (insurance firm) retains data locally within a secure enclave while contributing encrypted model updates to a global aggregator. The system ensures data privacy, fairness, and adaptive learning from diverse sources.

■■ Technical Implementation

- **Decentralized FL Setup:** Each insurer acts as an independent FL client, training locally on breach-related data (incidents, configurations, threat scans).
- **Federated Model Tasks:** Predict breach probability and expected financial loss from cyber incidents.
- **Differential Privacy:** Adds noise to gradients to prevent data reconstruction.
- **Secure Aggregation:** Cryptographic protection ensures only aggregate model updates are visible.

- **Asynchronous Updates:** Handles varied update intervals from insurers with different compute capabilities.
- **Robustness Against Poisoning:** Implements anomaly detection for malicious updates and model drift handling.

■ Breach Prediction Dataset & Features

For the breach prediction task, the model learns from diverse data points sourced from synthetic or anonymized datasets. Example features include:

- System configuration and vulnerability scores
- Threat intelligence feeds and patching history
- Incident logs and response time
- Firmographics: organization size, industry type, geographic exposure
- Loss history and claim frequency

■ The Adaptive Learning Utility (ALU) Score

The **ALU Score** introduces a domain-agnostic evaluation framework for Federated Learning systems. It measures not just model accuracy but learning behavior and collaboration quality.

- **Learning Efficiency:** Measures improvement rate per communication round.
- **Data Contribution Utility:** Quantifies how much each client's data improves model generalization.
- **Noise Robustness:** Evaluates system stability against differential privacy noise or adversarial updates.
- **Fairness Factor:** Balances performance gains with each client's participation level.
- **Dynamic Adaptation:** Scores the system's ability to handle non-IID and drifting client data.

■ System Design & Tooling

Fed-CyRA can be implemented using frameworks like **Flower**, **TensorFlow Federated**, or **PySyft**. Each insurer node trains local models using synthetic datasets, exchanges encrypted gradients, and contributes to a global aggregation server. A visualization dashboard presents the global risk heatmap and ALU-based system evaluation.

■ Why Fed-CyRA Stands Out

- Transforms competition into collaboration through privacy-preserving intelligence sharing.
- Defines a new evaluation paradigm (ALU Score) beyond traditional FL metrics.
- Scalable to any privacy-critical domain — finance, healthcare, or defense.
- Balances technical sophistication with real-world economic impact.
- Showcases mastery in federated systems, differential privacy, and adaptive metrics — aligning perfectly with the hackathon's theme.

Fed-CyRA is not just a federated learning prototype — it's a blueprint for the future of collaborative cybersecurity intelligence. It embodies fairness, trustlessness, and adaptive learning — the pillars of next-generation privacy-preserving distributed systems.