# Verifiable Federated Learning for Climate Risk Forecasting in MENA

Climate risk forecasting is vulnerable, inaccurate, and challenging in regions such as MENA due to limitations in data accessibility, privacy concerns, and unverified AI systems. Existing central AI models are often opaque, raising trust concerns, particularly in cross-border or post-conflict areas.

Therefore, I propose using verifiable federated learning to build a prediction system. A verifiable federated learning (FL) pipeline would help with early warnings of heatwave events, flood, and climate changes. Additionally, it complies with the Nexus Observatory Protocol (OP) architecture. The key concept of the system is that it enables distributed nodes (e.g., municipal weather stations, IoT gateways, and NGOs) to collaboratively train AI models without having to share their data to a central datacenter. The trained model updates will be exchanged with the aggregation server securely as it will run in a Trust Execution Environments (TEEs), and verification of each update will be performed via zero-knowledge proofs (ZKPs) for cryptographic integrity.

The project would integrate historical weather data (NOAA/MSC), satellite imagery (Sentinel-2), and ground-level sensors to support risk prediction using a Pytorch-based Neural Network (NN). The audit process will be performed using NEChain for all the forecasts and model versions, additionally stakeholder-specific risk dashboards will be supported via output simulations.

By the end of 3 months, aimed deliverables include:

* A federated training simulation with sample data.
* Secure aggregation and output hashing.
* A mock ZK proof system to simulate verifiable model behavior.
* Documentation aligned with OP’s verifiable AI and DRR standards.

This project provides a scalable foundation for privacy-aware, trusted risk forecasting in climate-sensitive areas and zones. It also contributes directly to Nexus OP’s mission for decentralized, resilient disaster governance.