Federated Learning, Privacy & Secure Aggregation — Hands-on

Design and operate federated learning workflows for biomedical and omics projects where data stays at source. This module covers federated learning architectures, privacy risks, secure aggregation, basic differential privacy and governance patterns for multi site collaborations in R and Python ecosystems.

Federated Learning, Privacy & Secure Aggregation

Help Desk · WhatsApp

Session Index

Session 1

Fee: Rs 8800 Apply Now

Federated Learning Concepts & Architectures

Why federated learning for health and omics

data locality and regulatory constraints **multi hospital and multi lab collaborations** **comparison with centralised training**

Core FL architectures and workflows

cross silo vs cross device FL **server client**

orchestration loops | federated averaging idea (FedAvg style)

System design considerations for FL projects

network constraints and update cadence | client dropouts and robustness | logging and monitoring at sites

Session 2

Fee: Rs 11800 Apply Now

Privacy Threats, Secure Aggregation & DP Basics

Threat models in federated learning

gradient leakage intuition | membership inference attacks overview | honest but curious server perspective

Secure aggregation building blocks

masking and pairwise secrets idea | aggregate without seeing individual updates | robustness to client drop out in aggregation

Differential privacy (DP) intuition for FL

epsilon, delta and sensitivity ideas | noise addition to gradients or updates | utility vs privacy tradeoff thinking

Session 3

Fee: Rs 14800 Apply Now

FL for Omics & Clinical Data, Non IID Handling

Data heterogeneity in real FL deployments

non IID feature and label distributions | site specific protocols and instruments | class imbalance across hospitals

Algorithmic tweaks for non IID data

re weighting and per site learning rates | personalised models vs single global model | simple FedProx style regularisation idea

Case examples with omics and clinical features

federated risk prediction using EHR covariates | distributed omics signatures across labs | constraints on feature sharing and harmonisation

Session 4

Fee: Rs 18800 Apply Now

Evaluation, Governance & Deployment Patterns

Evaluating FL models fairly across sites

site wise vs pooled metrics | calibration and fairness per cohort | communication and compute cost tracking

Governance, agreements and audit trails

roles of coordinating and participating sites | logging model updates and versions | alignment with ethics and data privacy boards

Deliverables: FL pilot design and report pack

architecture diagram and protocol outline | R or Python prototype scripts for FL loop | risk and mitigation summary for stakeholders