Federated Learning and Data Privacy Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The explosive growth of Big Data and increasingly stringent global regulations like GDPR and CCPA have created a critical deadlock for enterprises: how to leverage powerful Machine Learning models without compromising sensitive user data. Traditional centralized data aggregation is now a significant compliance and security liability. Federated Learning (FL) emerges as the revolutionary Privacy-Preserving AI paradigm, shifting the data-centric training model to a decentralized, collaborative one. This course will immerse you in the foundational principles, advanced algorithms, and real-world deployment of FL, transforming raw data concerns into secure, distributed intelligence across Edge Computing environments.

Federated Learning and Data Privacy Training Course focuses on the practical application of cutting-edge Cryptographic Primitives like Differential Privacy (DP) and Homomorphic Encryption (HE), which are essential for securing model updates against sophisticated Inference Attacks. Participants will gain hands-on experience with industry-leading frameworks like TensorFlow Federated (TFF) and PySyft, and critically analyze the trade-offs between model Utility and Privacy Loss. By mastering Non-IID Data challenges and building Robust Aggregation strategies, you will be equipped to design and implement compliant, high-performance FL solutions in sensitive sectors like Healthcare, Finance, and IoT.

Programme Curriculum

Federated Learning and Data Privacy Training Course

Introduction

The explosive growth of Big Data and increasingly stringent global regulations like GDPR and CCPA have created a critical deadlock for enterprises: how to leverage powerful Machine Learning models without compromising sensitive user data. Traditional centralized data aggregation is now a significant compliance and security liability. Federated Learning (FL) emerges as the revolutionary Privacy-Preserving AI paradigm, shifting

the data-centric training model to a decentralized, collaborative one. This course will immerse you in the foundational principles, advanced algorithms, and real-world deployment of FL, transforming raw data concerns into secure, distributed intelligence across Edge Computing environments.

Federated Learning and Data Privacy Training Course focuses on the practical application of cutting-edge Cryptographic Primitives like Differential Privacy (DP) and Homomorphic Encryption (HE), which are essential for securing model updates against sophisticated Inference Attacks. Participants will gain hands-on experience with industry-leading frameworks like TensorFlow Federated (TFF) and PySyft, and critically analyze the trade-offs between model Utility and Privacy Loss. By mastering Non-IID Data challenges and building Robust Aggregation strategies, you will be equipped to design and implement compliant, high-performance FL solutions in sensitive sectors like Healthcare, Finance, and IoT.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Architect and deploy Cross-Device and Cross-Silo Federated Learning systems.
2. Implement and fine-tune Federated Averaging (FedAvg) and advanced FL algorithms for Statistical Heterogeneity (Non-IID).
3. Apply Differential Privacy (DP) techniques to quantify and manage Privacy Loss during model training.
4. Utilize Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMC) for Secure Aggregation of model updates.
5. Mitigate advanced security risks, including Model Inversion Attacks and Membership Inference Attacks.
6. Ensure GDPR and CCPA Compliance through the practical use of Privacy-Enhancing Technologies (PETs).
7. Optimize FL systems for Communication Efficiency and scalability in Edge AI deployments.
8. Design Byzantine-Robust FL protocols to defend against malicious and unreliable client contributions.
9. Evaluate the critical Utility-Privacy Trade-off and select appropriate hyperparameters.
10. Integrate FL with Trusted Execution Environments (TEEs) for enhanced hardware-level security.
11. Develop and test FL models using TensorFlow Federated (TFF) and/or PySyft/OpenMined frameworks.
12. Analyze real-world Case Studies in Healthcare AI and Financial Fraud Detection.
13. Formulate a comprehensive Responsible AI strategy encompassing data lineage, fairness, and privacy in distributed systems.

Target Audience

1. Machine Learning Engineers and Data Scientists.
2. AI Researchers and Academics.
3. Data Privacy Officers (DPOs) and Compliance Managers.
4. Security and Cloud Architects.
5. Software Engineers.
6. Product Managers.
7. Ethical AI Specialists and Responsible AI Developers.
8. CTOs and Technical Leaders.

Course Modules

Module 1: Introduction to FL and the Data Privacy Imperative

- Big Data value and GDPR/CCPA regulatory risks.
- Centralized and Distributed ML.
- Cross-Silo FL, Cross-Device FL, Statistical & System Heterogeneity.
- Anatomy of a FL communication round.
- Case Study: Google's Predictive Text on mobile devices

Module 2: The Core Algorithm and Statistical Challenges

- Deep dive into Federated Averaging and its convergence properties.
- Addressing the Non-IID Data challenge
- Techniques for client sampling and selection
- Communication optimization: gradient compression and update quantization.
- Case Study: Improving Health Diagnosis across multiple hospitals with diverse patient populations

Module 3: Differential Privacy (DP) for Federated Learning

- The rigorous, mathematical foundation of ϵ-Differential Privacy.
- Implementing DP-SGD for local model updates.
- Utility vs. Privacy Loss trade-off: calibrating the ϵ budget.
- Advanced DP techniques.
- Case Study: Anonymizing Network Traffic Logs for intrusion detection while meeting a strict ϵ requirement.

Module 4: Cryptographic Privacy-Enhancing Technologies (PETs)

- Introduction to Secure Multi-Party Computation for joint function computation.
- Using SMC for Secure Aggregation.
- Fundamentals of Homomorphic Encryption
- Applying HE for model update aggregation without server decryption.
- Case Study: Cross-Bank Anti-Money Laundering detection using SMC for secure transaction pattern analysis.

Module 5: Security Threats and Robustness in FL

- Understanding Model Inversion Attacks and their goal of reconstructing training data.
- Mitigating Membership Inference Attacks to protect individual participation status.
- Defense against adversarial clients.
- Implementing Byzantine-Robust Aggregation algorithms.
- Case Study: IoT Device Security where a few compromised devices attempt to poison the global malware detection model.

Module 6: FL Frameworks and Practical Implementation

- In-depth Hands-On with TensorFlow Federated (TFF) for large-scale production.
- Utilizing PySyft and the OpenMined ecosystem for experimentation and research.
- Simulating FL environments for benchmarking and optimization.
- Setting up client-server architectures and communication protocols.
- Case Study: Building a Federated Recommendation System using TFF for a personalized retail application.

Module 7: Deployment, Operations, and Edge AI

- MLOps principles in a distributed environment.
- Integrating FL with Trusted Execution Environments like Intel SGX.
- Managing System Heterogeneity.
- Best practices for model versioning, auditing, and decentralized governance.
- Case Study: Automotive Industry Autonomous Driving, updating models across vehicle fleets with low-latency and TEE-level security.

Module 8: Responsible AI and Future Trends

- The interplay of FL, Fairness, and Bias in decentralized datasets.
- FL and data provenance.
- Split Learning, Decentralized FL with Blockchain.
- The ethical considerations of using PETs in high-stakes decisions.
- Case Study: Addressing Algorithmic Bias in a federated credit scoring model across different demographic regions.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com