Training Course on Privacy-Preserving Machine Learning

Professional Development Training Course Outline

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

Course Introduction

In an era defined by **Big Data** and increasing **data privacy regulations** like GDPR and CCPA, the need for robust **Privacy-Preserving Machine Learning (PPML)** techniques has become paramount. Training Course on Privacy-Preserving Machine Learning delves into the cutting-edge methodologies that enable organizations to unlock the full potential of their data for advanced analytics and AI model development, all while ensuring the **confidentiality**, **security**, and **ethical handling** of sensitive information. Participants will gain practical expertise in **Federated Learning (FL)**, **Differential Privacy (DP)**, and **Homomorphic Encryption (HE)**, empowering them to build **secure AI solutions** that uphold **user trust** and maintain **regulatory compliance**.

This program offers a deep dive into the theoretical foundations and practical applications of PPML, addressing critical challenges in **decentralized AI**, **data anonymization**, and **secure computation**. Through hands-on exercises and real-world **case studies**, attendees will learn to implement and evaluate these advanced techniques, transforming how they approach **sensitive data analytics**, **collaborative AI**, and **AI model security**. Prepare to lead the charge in developing **privacy-first AI systems** that are both powerful and responsible.

Programme Curriculum

Training Course on Privacy-Preserving Machine Learning (PPML): Federated Learning, Differential Privacy, Homomorphic Encryption

Introduction

In an era defined by **Big Data** and increasing **data privacy regulations** like GDPR and CCPA, the need for robust **Privacy-Preserving Machine Learning (PPML)** techniques has become paramount. Training Course on Privacy-Preserving Machine Learning delves into the cutting-edge methodologies that enable organizations to unlock the full potential of their data for advanced

analytics and AI model development, all while ensuring the **confidentiality**, **security**, and **ethical handling** of sensitive information. Participants will gain practical expertise in **Federated Learning (FL)**, **Differential Privacy (DP)**, and **Homomorphic Encryption (HE)**, empowering them to build **secure AI solutions** that uphold **user trust** and maintain **regulatory compliance**.

This program offers a deep dive into the theoretical foundations and practical applications of PPML, addressing critical challenges in **decentralized AI**, **data anonymization**, and **secure computation**. Through hands-on exercises and real-world **case studies**, attendees will learn to implement and evaluate these advanced techniques, transforming how they approach **sensitive data analytics**, **collaborative AI**, and **AI model security**. Prepare to lead the charge in developing **privacy-first AI systems** that are both powerful and responsible.

Course Duration

5 days

Course Objectives

1. Understand the fundamental principles of Privacy-Preserving Machine Learning, including its motivations, challenges, and landscape.
2. Gain proficiency in designing and deploying Federated Learning architectures for decentralized model training.
3. Learn to integrate Differential Privacy mechanisms to achieve provable privacy guarantees in data analysis and model outputs.
4. Explore the capabilities of Homomorphic Encryption for performing computations on encrypted data without decryption.
5. Analyze the inherent trade-offs between privacy, accuracy, and computational efficiency in PPML techniques.
6. Understand the implications of data privacy regulations (e.g., GDPR, HIPAA, CCPA) on ML workflows and how PPML ensures adherence.
7. Discover diverse industry use cases for PPML across sectors like healthcare, finance, smart cities, and IoT.
8. Design and implement end-to-end secure machine learning pipelines that integrate various PPML methods.
9. Learn to identify and mitigate potential privacy risks and vulnerabilities in traditional ML systems.
10. Gain hands-on experience with popular PPML frameworks such as TensorFlow Federated, PySyft, and Microsoft SEAL.
11. Understand the principles and applications of SMPC for collaborative, privacy-preserving data analysis.
12. Develop strategies to balance data utility with strong privacy guarantees in practical scenarios.
13. Prepare for emerging trends and the evolving landscape of ethical AI and responsible data stewardship.

Organizational Benefits

- Drastically reduce the risk of **data breaches** and **sensitive information leakage** by processing data in a privacy-preserving manner.
- Proactively meet stringent **data privacy regulations** (GDPR, HIPAA, CCPA), avoiding costly fines and reputational damage.

- Safely leverage previously inaccessible or sensitive datasets for analysis and model training, fostering **data collaboration** without compromising privacy.
- Demonstrate a strong commitment to **data protection**, building **customer loyalty** and trust in AI-powered services.
- Lead the market with **privacy-by-design AI solutions**, fostering ethical innovation and responsible AI development.
- Enable **secure data sharing** and **collaborative model training** across different entities, even with highly sensitive data.
- Cultivate a culture of **responsible AI**, aligning with growing demands for ethical considerations in data handling and algorithm development.
- Minimize legal and reputational costs associated with privacy incidents and non-compliance.

Target Audience

1. Machine Learning Engineers & Data Scientists.
2. AI Researchers & Developers.
3. Data Privacy Officers (DPOs) & Compliance Teams
4. Security Architects & Engineers.
5. Cloud Architects & Engineers.
6. Product Managers (AI/ML focused).
7. Data Analysts & Statisticians.
8. Anyone Handling Sensitive Data.

Course Outline

Module 1: Introduction to Privacy-Preserving Machine Learning (PPML)

- Defining PPML: Concepts, motivations, and the privacy-utility dilemma.
- The evolving landscape of data privacy regulations: GDPR, HIPAA, CCPA, and their impact on ML.
- Key privacy threats in traditional ML: Model inversion, membership inference, attribute inference.
- Overview of core PPML paradigms: Federated Learning, Differential Privacy, Homomorphic Encryption, Secure Multi-Party Computation.
- **Case Study**: A healthcare provider leveraging PPML to comply with HIPAA regulations while collaboratively training diagnostic models across multiple hospitals.

Module 2: Federated Learning (FL)

- Fundamentals of Federated Learning: Decentralized training, model aggregation, and communication protocols.
- Types of Federated Learning: Horizontal, Vertical, and Federated Transfer Learning.
- Algorithms and frameworks for FL: Federated Averaging (FedAvg), TensorFlow Federated, PySyft, Flower.
- Challenges in FL: Data heterogeneity (Non-IID data), client selection, communication efficiency.
- **Case Study**: Google's use of Federated Learning for Gboard predictive text, training models on user data without sending raw data to the cloud.

Module 3: Differential Privacy (DP)

- Mathematical foundations of Differential Privacy: ?-DP, ?-DP, and their interpretations.
- Adding calibrated noise: Laplace and Gaussian mechanisms for achieving DP.

- DP in data release: Private query answering, synthetic data generation.
- DP in model training: Differentially private Stochastic Gradient Descent (DP-SGD) and its applications.
- **Case Study**: The U.S. Census Bureau's adoption of Differential Privacy for releasing decennial census data to protect individual respondent privacy.

Module 4: Homomorphic Encryption (HE)

- Introduction to Cryptography and Encryption basics.
- Types of Homomorphic Encryption: Partially HE (PHE), Somewhat HE (SHE), and Fully HE (FHE).
- Understanding encryption schemes: BGV, BFV, CKKS, and their suitable operations.
- Performing computations on encrypted data: Addition, multiplication, and more complex operations.
- **Case Study**: IBM's research on applying machine learning directly to fully encrypted banking data for fraud detection, demonstrating equivalent accuracy to models on unencrypted data.

Module 5: Secure Multi-Party Computation (SMPC)

- Principles of SMPC: Secret sharing, garbled circuits, and oblivious transfer.
- SMPC protocols for secure collaborative analysis without revealing individual inputs.
- Combining SMPC with other PPML techniques for enhanced privacy.
- Practical considerations for SMPC: Communication overhead, computational cost, and scalability.
- **Case Study**: Financial institutions using SMPC to collaboratively analyze financial transactions for anti-money laundering (AML) efforts without exposing individual transaction details.

Module 6: Advanced PPML Topics & Hybrid Approaches

- Combining FL with DP: Enhancing privacy in federated settings.
- Integrating HE with FL and DP: Enabling computations on encrypted gradients or models.
- Trusted Execution Environments (TEEs): Hardware-based privacy guarantees.
- Emerging trends in PPML: Zero-Knowledge Proofs (ZKPs) and their potential.
- **Case Study**: A consortium of research institutions combining Federated Learning with Differential Privacy to analyze rare disease data, pooling insights while protecting patient confidentiality.

Module 7: Implementation & Tools for PPML

- Hands-on exercises with TensorFlow Federated for FL model development.
- Implementing Differential Privacy using Opacus (PyTorch) or TensorFlow Privacy.
- Working with Homomorphic Encryption libraries: Microsoft SEAL, TenSEAL, HElib.
- Setting up secure development environments and best practices for PPML deployment.
- **Case Study**: Developing a sentiment analysis model using a combination of Federated Learning and Homomorphic Encryption to protect user review data on a mobile platform.

Module 8: PPML Applications, Ethics & Future Directions

- Deep dive into PPML applications in specific industries: Healthcare diagnostics, financial fraud detection, personalized advertising, smart city planning, IoT data processing.
- Ethical considerations in PPML: Fairness, bias, accountability, and explainability.

- Challenges and open research problems in PPML scalability, interpretability, and practical deployment.
- Regulatory outlook and the future of data privacy and AI.
- **Case Study**: A smart city initiative using PPML techniques to analyze traffic patterns and optimize public transport routes, ensuring citizen privacy while improving urban mobility.

Training Methodology

This course will employ a dynamic and interactive training methodology designed to maximize learning and practical application. It will include:

- **Instructor-led lectures**: Clear and concise explanations of theoretical concepts.
- **Hands-on coding exercises**: Practical implementation of PPML algorithms using Python and relevant frameworks (TensorFlow Federated, PySyft, Opacus, Microsoft SEAL).
- **Live demonstrations**: Walkthroughs of complex PPML setups and solutions.
- **Case study analysis**: In-depth discussions of real-world applications and challenges.
- **Group discussions & problem-solving**: Collaborative learning and critical thinking.
- **Q&A sessions**: Opportunities for clarification and deeper understanding.
- **Project-based learning**: Participants will work on a capstone project to apply learned concepts.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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