Federated Machine Learning

Code: CS31223CS	Course Type: Elective	Semester: II
Evolution Scheme (TA-MSE-ESE): 20-30-100	Total Marks: 150	L-T-P (Credits): 3-0-0 (3)

Pre-Requisites: Machine Learning, Basic Computer Systems, and Basic ProgrammingSkills.

Course Objective: To understand federated learning architectures, theoretical foundations, core algorithms, and diverse frameworks for privacy-preserving distributed machine learning applications across vision, language, recommendation, and related domains.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Explain the fundamentals, architecture, and privacy foundations of Federated Learning.
CO-2	Describe distributed learning principles, security challenges, and emerging research trends in Federated Learning.
CO-3	Analyze horizontal, vertical, and transfer federated learning models and core algorithms.
CO-4	Illustrate the significance of Federated Learning in vision, language, recommendation, and other emerging applications.

Course Articulation Matrix:

PO	PEO-1	PEO-2	PEO-3	PEO-4	PEO-5
CO-1	2	2	1	1	2
CO-2	2	3	1	1	3
CO-3	3	3	1	1	2
CO-4	2	2	1	1	2

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Foundations of Federated Learning

Motivation, Definition, Need for Federated Learning, Categories of FL, FL workflow and architecture, current developments, research issues, open-source platforms, standardization efforts, federated AI ecosystem.

Unit-2: Privacy and Distributed Learning Foundations

Distributed Machine Learning overview, scalability and privacy motivations, privacy-preserving machine learning, threat and security models, privacy-preserving techniques, secure multi-party computation, homomorphic encryption, differential privacy, vanilla federated learning.

Unit-3: Federated Learning Models and Algorithms

Horizontal Federated Learning, architecture, client-server and peer-to-peer settings, global model evaluation, FedAvg algorithm, communication efficiency, client selection.

VerticalFederated Learning: concepts, architecture, secure linear regression, secure tree boosting. Federated Transfer Learning: concept, framework, training and prediction process.

Unit-4: Applications and Emerging Trends

Federated Learning for Computer Vision, NLP, and Recommendation Systems. Introduction to Federated Reinforcement Learning. Recent research trends, challenges, fairness, personalization, security, and real-world applications.

Learning Resources:

1. H. Brendan McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," AISTATS, 2017.
2. Dou et al., "Federated deep learning for detecting COVID-19 lung abnormalities in CT," *npj Digital Medicine*, 2021.
3. https://www.persistent.com/blogs/privacy-preserving-ai-private-ai-the- rise-of-federated-learning/
4. https://research.aimultip1e.com/federated-learning/
5. https://towardsdatascience.com

Text Books:

1. Federated Learning, Qiang Yang, Yang Liu, Yong Cheng, Yan Kang, Tianjian Chen, and Han Yu Synthesis Lectures on Artificial Intelligence and Machine Learning 2019.
2. Federated Learning with Python by Kiyoshi Nakayama PhD, George Jeno , O'Reilly Media, Inc. Pub.
3. .What-is-federated learning? By Emily Glanz, Nova Fallen, O'Reilly Media, Inc. Pub.