Federated Machine Learning

Code: CS32222CS	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 Programming Skills.

Course Objective:

1. Understand the key concepts, architecture, and challenges of Federated Learning.
2. Learn the theoretical foundations and core algorithms of Federated Learning.
3. Analyze horizontal, vertical, and transfer federated learning frameworks.
4. Explore recent research trends and applications of Federated Learning in vision, language, recommendation, and related domains.

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

CO-1	Explain the principles, architecture, and privacy foundations of Federated Learning, including distributed learning workflows and federated AI ecosystems.
CO-2	Analyze distributed learning frameworks, security threats, and privacy-preserving techniques such as secure multi-party computation, homomorphic encryption, and differential privacy in Federated Learning systems.
CO-3	Apply horizontal, vertical, and transfer Federated Learning algorithms, including FedAvg and secure federated optimization methods, to design privacy-aware distributed learning models.
CO-4	Evaluate Federated Learning applications in computer vision, NLP, recommendation systems, and emerging intelligent systems with consideration of fairness, personalization, scalability, and security challenges.

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. Vertical

Federated 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. Qiang Yang, Yang Liu, Yong Cheng, Yan Kang, Tianjian Chen, and Han Yu, Federated Learning, Synthesis Lectures on Artificial Intelligence and Machine Learning, First Edition, Morgan & Claypool Publishers / Springer Nature, 2019, ISBN: 978-1681736983 / 978-3031004575
2. Kiyoshi Nakayama and George Jeno, Federated Learning with Python: Design and Implement a Federated Learning System and Develop Applications Using Existing Frameworks, First Edition, Packt Publishing, 2022, ISBN: 978-1803247106 / 978-1803248752
1. Emily Glanz and Nova Fallen, What Is Federated Learning?, First Edition, O'Reilly Media, Inc., 2022, ISBN: 978-1098118624