Federated Learning

Code: CS33321CS	Course Type: Core	Semester: III
Evolution Scheme (TA-MSE-ESE): 20-30-100	Total Marks: 150	L-T-P (Credits): 3-0-0 (3)

Pre-Requisites:

- Fundamentals of Machine Learning
- Basic knowledge of Distributed Systems
- Mathematics: Linear Algebra, Probability, Optimization
- Programming knowledge (Python preferred)
- Basic understanding of Data Privacy and Security

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

CO-1	Understand the concepts, architecture, and challenges of Federated Learning systems.
CO-2	Analyze and apply privacy-preserving techniques in distributed machine learning environments.
CO-3	Design and implement federated learning models using HFL, VFL, and FTL approaches.
CO-4	Evaluate optimization strategies, communication efficiency, and security in FL frameworks.
CO-5	Apply federated learning in real-world applications such as vision, NLP, recommendation, and reinforcement learning.

Course Articulation Matrix:

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

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Introduction and Privacy Foundations: Introduction: Motivation, Federated Learning as a Solution, The Definition of Federated Learning, Categories of Federated Learning, Current Development in Federated Learning, Research Issues in Federated Learning, Open-Source Projects, Standardization Efforts, The Federated AI Ecosystem; Background: Privacy Preserving Machine Learning, PPML and Secure ML, Threat

and Security Models, Privacy Threat Models, Adversary and Security Models, Privacy Preservation Techniques, Secure Multi-Party Computation, Homomorphic Encryption, Differential Privacy.

Unit-2: Distributed and Privacy-Preserving Machine Learning: Distributed Machine Learning: Introduction to DML, The Definition of DML, DML Platforms, Scalability- Motivated DML, Large-Scale Machine Learning, Scalability-Oriented DML Schemes, Privacy-Motivated DML, Privacy-Preserving Decision Trees, Privacy Preserving Techniques, Privacy-Preserving DML Schemes, Privacy-Preserving Gradient Descent, Vanilla Federated Learning, Privacy-Preserving Methods.

Unit-3: Federated Learning Architectures and Algorithms: Horizontal Federated Learning: The Definition of HFL, Architecture of HFL, The Client Server Architecture, The Peer-to-Peer Architecture, Global Model Evaluation, The Federated Averaging Algorithm, Federated Optimization, The FedAvg Algorithm, The Secured FedAvg Algorithm, Improvement of the FedAvg Algorithm, Communication Efficiency, Client Selection; Vertical Federated Learning: The Definition of VFL, Architecture of VFL, Algorithms of VFL, Secure Federated Linear Regression, Secure Federated Tree-Boosting.

Unit-4: Advanced Federated Learning Techniques: Federated Transfer Learning: Heterogeneous Federated Learning, Federated Transfer Learning, The FTL Framework, Additively Homomorphic Encryption, The FTL Training Process, The FTL Prediction Process, Security Analysis, Secret Sharing Based FTL Incentive Mechanism Design for Federated Learning: Paying for Contributions, Profit- Sharing Games, Reverse Auctions, A Fairness-Aware Profit Sharing Framework, Modeling Contribution, Modeling Cost, Modeling Regret, Modeling Temporal Regret, The Policy Orchestrator, Computing Payoff Weightage.

Unit-5: Applications and Emerging Trends

Federated Learning for Vision, Language, and Recommendation: Federated Learning for Computer Vision, Federated CV, Federated Learning for NLP, Federated NLP, Federated Learning for Recommendation Systems, Recommendation Model, Federated Recommendation System Federated Reinforcement Learning: Introduction to Reinforcement Learning, Policy, Reward, Value Function, Model of the Environment, RL Background Example, Reinforcement Learning Algorithms, Distributed Reinforcement Learning, Asynchronous Distributed Reinforcement Learning, Synchronous Distributed Reinforcement Learning, Federated Reinforcement Learning, Background and Categorization; Recent trends and future. directions in FL.

Learning Resources:

Textbooks:

1. Q. Yang, L. Fan, and H. Yu, *Federated Learning*, Springer, 2020.
2. L. M. Nguyen, T. N. Hoang, and P.-Y. Chen, *Federated Learning: Theory and Practice*, Elsevier, 2024.

Reference Book:

1. H. Ludwig and N. Baracaldo, *Federated Learning: Methods and Applications*, Springer, 2022.
2. S. Sahoo et al., *Federated Learning: Principles, Paradigms, and Applications*, CRC Press, 2024.