DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

NATIONAL INSTITUTE OF TECHNOLOGY PATNA

Ashok Raj Path, PATNA 800 005 (Bihar), India

Phone No.: 0612 – 2372715, 2370419, 2370843, 2371929, 2371930, 2371715 Fax – 0612- 2670631 Website: www.nitp.ac.in

CSXX2847 Federated Learning

L-T-P-Cr: 3-0-0-3

Pre-requisites: Machine Learning

Objectives/Overview:

- To introduce various topics of Federated Machine learning along with their applications.

Course Outcomes:

At the end of the course, a student will be able to understand:

Sl. No	Course Outcome (CO)	Mapping to POs
1.	The basic concepts and need of federated machine learning (FML)	PO1, PO2
2.	The privacy preservation techniques in FML	PO1, PO3
3.	The concepts and techniques of distributed machine learning	PO1, PO2,PO3
4.	The concepts and techniques of horizontal and vertical federated learning	PO1, PO2,PO3, PO4
5.	The techniques of using SVM and neural n/w in FML	PO1, PO2, PO3, PO4, PO5
6.	The use of federated learning in the field of Computer Vision	PO1, PO2, PO3, PO4, PO5

UNIT I: Introduction to Federated Machine Learning (FML) Lectures: 05

Motivation; Federated Learning as a Solution: Definition, Categories; Current development in Federated Learning: Research issues, Open-source projects, Standardization efforts, Federated AI ecosystem.

UNIT II: Privacy preservation in FML Lectures: 07

Privacy-preserving Machine Learning (PPML); 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 III: Distributed Machine Learning (DML) Lectures: 10

Introduction to DML: Definition, 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 IV: Horizontal and Vertical Federated Learning Lectures: 10

Definition, Architecture of Horizontal Federated Learning: Client-server architecture, Peer-to-peer architecture, Global model evaluation; Federated Averaging Algorithm: Federated optimization, FedAvg algorithm, Secured FedAvg algorithm; Improvement of FedAvg algorithm: Communication efficiency, Client selection; Definition of Vertical Federated Learning (VFL), Architecture of VFL, Algorithms of VFL: Secure federated linear regression, Secure federated tree boosting.

UNIT V: Support Vector Machine and Neural Network in FML Lectures: 06

SVM overview, Privacy-preserving SVM over vertically partitioned data, Privacy-preserving SVM over horizontally partitioned data, Privacy-preserving SVM over arbitrarily partitioned data, Neural N/W overview, Privacy-preserving Neural N/W over vertically partitioned data, Privacy-preserving Neural N/W over horizontally partitioned data, Privacy-preserving Neural N/W over arbitrarily partitioned data.

UNIT VI: Federated Learning for Computer Vision Lectures: 04

Federated learning for Computer Vision: Federated CV, Related works, Challenges; Federated Transfer Learning (FTL): FTL framework, Additively homomorphic encryption, FTL training process, FTL prediction process, Security analysis.

.

Text/Reference Books

1. Q. Yang, Y. Liu, Y. Cheng, Y. Kang, T. Chen, H. Yu, "Federated Learning", Morgan & Claypool Publishers.
2. H. Ludwig, N, Baracaldo, “ Federated Learning: A Comprehensive Overview of Methods and Applications”, Springer.