NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	BTech (CSE)
Course Code:	3CS110ME24
Course Title:	Federated Learning
Course Type:	Disciplinary Minor-Elective
Year of Introduction:	2024-25

L	**T**	**Practical Component**				**C**
		LPW	**PW**	**W**	**S**	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. explain the fundamentals of federated learning (BL2)
2. make use of techniques of federated learning for developing various applications (BL3)
3. list real-world applications and use cases of federated learning
4. discuss the privacy and security considerations in federated learning. (BL4)

(BL6)

Unit	**Contents**	**Teaching Hours (Total 45)**
Unit-I	**Introduction:** Empirical Probability, Theoretical Probability, Joint Probability, Bayes' Theorem, Descriptive Statistics, Measure of Center, Measure of Variability, Measure of Position, Data visualization, supervised and unsupervised learning	05
Unit-II	**Regression Techniques:** Basic concepts and applications of Regression, Simple Linear Regression – Gradient Descent and Normal Equation Method, Multiple Linear Regression, Non-Linear Regression, Linear Regression with Regularization, Hyper-parameters tuning, Loss Functions, Evaluation Measures for Regression Techniques, Artificial neural network, Perceptron Learning, Activation Functions, Multilayer Perceptrons.	12
Unit-III	**Introduction to Federated Learning:** Concept of federated learning, Motivations and advantages, Federated learning as a solution, Current development in federated learning.	08
Unit-IV	**Distributed Machine learning:** Introduction to DML, scalability, privacy in DML, privacy-preserving gradient descent. Horizontal federated learning, architecture of HFL, Vertical federated learning, architecture of VFL	06
Unit-V	**Federated Learning Algorithms:** Federated Averaging, Federated Stochastic Gradient Descent (FSGD), Federated Learning with Differential Privacy, Other federated learning algorithms	04
Unit-VI	**Privacy and Security in Federated Learning:** Differential privacy and federated learning, Secure aggregation and encryption techniques, Threat models and mitigations, Real-world privacy breaches and lessons learned	06
Unit-VII	**Application:** Healthcare and medical research, Finance and fraud detection, Mobile and IoT applications, Federated learning in federated industries	04

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Qiang Yang Yu, Federated Learning, Morgan and Claypool
2. Muhammad Habib, Federated Learning Systems, Springer
3. Heiko Ludwig, Nathalie Baracaldo, Federated Learning: A Comprehensive Overview of
4. Methods and Applications, Springer
5. Roozbeh Razavi-Far, Boyu Wang, et al., Federated and Transfer Learning: (Adaptation, Learning, and Optimization), Springer

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Introduction to Python and Libraries o Set up a Python environment with popular libraries (e.g., NumPy, Pandas, Scikit-Learn). o Load a dataset and perform basic data manipulation tasks. o Explore Jupyter Notebooks for interactive coding.	02
2	Data Preprocessing and Visualization o Clean and preprocess a real-world dataset. o Visualize the data using Matplotlib and Seaborn. o Handle missing values, outliers, and feature scaling.	02
3	Supervised Learning - Regression o Build a simple linear regression model using Scikit-Learn. o Train and evaluate the model on a regression dataset. o Plot the regression line and assess model performance.	02
4	Setting Up a Federated Learning Environment o Install and configure the necessary libraries and tools for federated learning (e.g., TensorFlow, PyTorch). o Set up a basic federated learning environment. o Train a simple federated model on a synthetic dataset.	02
5	Federated Averaging Algorithm o Implement the Federated Averaging (FedAvg) algorithm. o Use FedAvg to train a basic model across decentralized data sources. o Evaluate the model's performance and compare it to a centralized model.	04
6	Implementing Federated Stochastic Gradient Descent (FSGD) o Implement Federated Stochastic Gradient Descent (FSGD). o Train a model using FSGD and compare its convergence with standard SGD. o Discuss the benefits and drawbacks of FSGD.	04
7	Differential Privacy in Federated Learning o Implement Federated Learning with Differential Privacy (DP). o Explore the impact of varying privacy parameters on model accuracy. o Discuss the trade-offs between privacy and utility.	02
8	Secure Aggregation and Encryption Techniques	04

	o Implement secure aggregation techniques (e.g., secure sum) in federated learning. o Encrypt and decrypt model updates for privacy. o Compare the performance of secure aggregation with non-secure methods.	
9	Federated Learning on Heterogeneous Data Sources o Simulate federated learning on datasets with varying distributions. o Explore techniques for handling non-IID (non-Independently and Identically Distributed) data. o Discuss strategies to mitigate issues with heterogeneous data sources.	04
10	Federated Transfer Learning o Implement federated transfer learning to leverage pre-trained models. o Fine-tune a pre-trained model on decentralized data sources. o Evaluate the transfer learning model's performance.	04