INSTITUTE OF AERONAUTICAL ENGINEERING
(Autonomous)
Dundigal - 500 043, Hyderabad, Telangana

COURSE CONTENT

FEDERATED MACHINE LEARNING								
VII Semester: CSE (AI&ML)								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
ACAD27	Elective	3	0	0	3	40	60	100
Contact Classes: 48	**Tutorial Classes: Nil**	**Practical Classes: Nil**				**Total Classes: 48**		
Prerequisites: Computational AI								

I. COURSE OVERVIEW:

Federated learning (often referred to as collaborative learning) is a decentralized approach to training machine learning models. It doesn't require an exchange of data from client devices to global servers. Instead, the raw data on edge devices is used to train the model locally, increasing data privacy. It covers Distributed Machine Learning, Horizontal Federated Learning and Federated Learning for Vision, Language, and Recommendation. Federated machine learning offers numerous substantial benefits, including enhanced user privacy and protection, adherence to regulatory compliance, improved accuracy and diversity in models, increased bandwidth efficiency, and greater scalability.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The key concepts and issues behind Federated Learning.
II. Key theoretical results of Federated Learning and Horizontal Federated Learning .
III. The concepts of Federated Learning for Vision, Language, and Recommendation.

III. COURSE OUTCOMES:

At the end of the course, student should be able to:

CO1 Make use of Federated Learning concepts to real-world scenarios, considering diverse data distributions and privacy requirements.
CO2 Outline the concept of transactions in databases, including the use of COMMIT and ROLLBACK statements to ensure data consistency and integrity.
CO3 Discuss problem-solving skills by addressing challenges related to data manipulation, query optimization, and maintaining data consistency.
CO4 Assume real-world applications and use cases where HFL is applicable. This could involve case studies, industry examples, or practical scenarios.
CO5 Utilize skills in documenting HFL implementations, communicating results, and potentially presenting findings to various stakeholders.
CO6 Interpret proficiency in using DML commands to perform common operations such as querying, inserting, updating, and deleting data.

IV. COURSE CONTENT:

MODULE – I: INTRODUCTION (10)

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.

MODULE – II: DISTRIBUTED MACHINE LEARNING (09)

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.

MODULE – III: HORIZONTAL FEDERATED LEARNING (09)

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.

MODULE – IV: FEDERATED LEARNING (10)

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.

MODULE – V: VISION, LANGUAGE, AND RECOMMENDATION (10)

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.

V. TEXTBOOKS:

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.

VI. REFERENCE BOOKS:

1. Federated Learning Systems: Towards Next-Generation AI, 1Muhammad Habib Ur Rehaman, Mohammad Medhat Gaber, Springer, 1st ed. 2021 Edition, Kindle Edition.
2. Federated Learning: A Comprehensive Overview of Methods and Applications, Heiko Ludwig, Nathalie Baracaldo, Springer Nature 7 Jul 2022.

VII. WEB REFERENCES

1. https://link.springer.com/book/10.1007/978-3-031-01585-4
2. https://link.springer.com/book/10.1007/978-981-19-7083-2
3. https://shop.elsevier.com/books/federated-learning/nguyen/978-0-443-19037-7

VIII. MATERIALS ONLINE

1. Course template
2. Tutorial question bank
3. Tech talk topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)