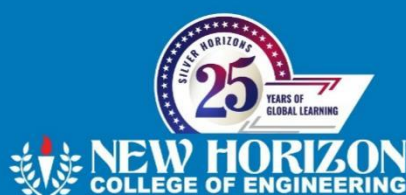# NEW HORIZON COLLEGE OF ENGINEERING

DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

EVENT –Technical Expert Talk on Federated Learning and Privacy Preserving in AI

Venue: Falconry Hall, NHCE   **Time: 9:30 AM to 11:30 AM**

Department of Artificial Intelligence and Machine Learning

Expert Talk

Federated Learning and Privacy Preserving in AI

📅 15 September 2025

🕘 09:30 AM - 11:30 AM

📍 Falconry Seminar Hall

👥 5th Sem Students

Mr. A J V Manumohan
Deloitte ADMM Analyst
Bengaluru

Student Coordinators

Prathyusha S   **Pranav P S**   **Lakshmi**   **Pranav P**

Faculty Coordinators

Dr. Sonia Maria D'Souza   **Dr. Akshatha P S**   **Prof. Sivashankari**   **Prof. Sindhuja**
Associate Professor   Senior Assistant Professor   Senior Assistant Professor   Senior Assistant Professor

Convenors

Dr. N V Uma Reddy   **Dr. Manjunatha**
HoD - AIML   Principal

Introduction

On the 15th of September 2025, the Falconry Seminar Hall at New Horizon College of Engineering (NHCE) hosted an insightful technical expert talk on "Federated Learning and Privacy Preserving in AI." The session was conducted by Mr. A J V Manumohan, Deloitte ADMM Analyst, Bengaluru. With his in-depth expertise in Artificial Intelligence and its industrial applications, Mr. Manumohan offered students valuable insights into modern methods of data privacy, distributed machine learning, and their practical significance. Held from 09:30 AM to 11:30 AM, the session was designed for 5th-semester students and proved both engaging and informative.

Session Overview

Mr. Manumohan structured the talk to emphasize the importance of data privacy in AI systems and introduced Federated Learning (FL) as a promising solution. He began with the fundamental question, "Why Machine Learning?" and discussed the limitations of traditional centralized training, where data from multiple sources is aggregated. He then presented Federated Learning as a paradigm in which models are trained collaboratively across devices or organizations without directly sharing sensitive data, thus preserving privacy while enabling collective intelligence in machine learning applications.

Key Topics Covered

1. Types of Machine Learning
- **Supervised Learning:** Defined with process, goals, and relatable analogies.
- **Unsupervised Learning:** Explained using *Market Basket Analysis* as a classic example.
- **Reinforcement Learning:** Illustrated through the analogy of a *self-driving car* improving by trial and error.

2. Machine Learning in Action
- How **Image Recognition** works: input → hidden layers → output.
- Applications such as *face unlock* and *voice recognition* were discussed to connect theory with daily life.

3. Challenges in Machine Learning
- Data quality and preprocessing difficulties.
- Requirement for large datasets.
- Biases in data and fairness concerns.
- Overfitting and underfitting issues.
- High computational cost and the "black box" nature of models.

Practical Demonstration

A significant part of the talk involved a **hands-on demonstration in Google Colab.** Students observed how to:
- Configure and standardize data.
- Build and compile a **basic Keras classification model.**
- Train the model and visualize progress.
- Identify and address **overfitting** using **data augmentation and dropout.**

The session also touched upon **Support Vector Machines (SVMs)**
- Definition of support vectors and hyperplanes.
- Applications of SVM in supervised classification tasks.

These demonstrations helped bridge the gap between theory and implementation.

Conclusion

The expert talk on "Federated Learning and Privacy Preserving in AI" by Mr. A J V Manumohan was an insightful session that provided students with a structured understanding of Machine Learning fundamentals and workflows. Although the interaction was limited, the session offered clarity on key ML concepts and practical exposure to model building.

At the conclusion of the session, the faculty coordinators extended their gratitude by presenting a token of appreciation to the speaker. This thoughtful gesture marked the end of a meaningful and enriching session that inspired students to further explore Machine Learning.

Feedback Report

The technical expert talk on "Federated Learning and Privacy Preserving in AI," conducted by Mr. A J V Manumohan on 15th September 2025, received an overwhelmingly positive response from participants. Students appreciated the clarity of explanations, the structured flow of concepts, and the hands-on demonstration using Google Colab, which made the learning experience more engaging. Many noted that the session enhanced their understanding of supervised, unsupervised, and reinforcement learning, while also introducing them to practical applications such as image classification and SVMs.

Overall, the talk was considered highly informative, relevant, and motivating, with most students rating it Excellent or Good.

Feedback Summary