
# UE21CS343BB2

# Topics in Deep Learning

## Categorization of Federated Learning

**Dr. Shylaja S S**
Director of Cloud Computing & Big Data (CCBD), Centre for Data Sciences & Applied Machine Learning (CDSAML)
Department of Computer Science and Engineering
**shylaja.sharath@pes.edu**

**Ack: Divya K,**
**Teaching Assistant**

# Topics in Deep Learning

## Overview


- Introduction
- Horizontal Federated Learning
- Vertical Federated Learning’
- Federated Transfer Learning (FTL)
- Conclusion

## Introduction

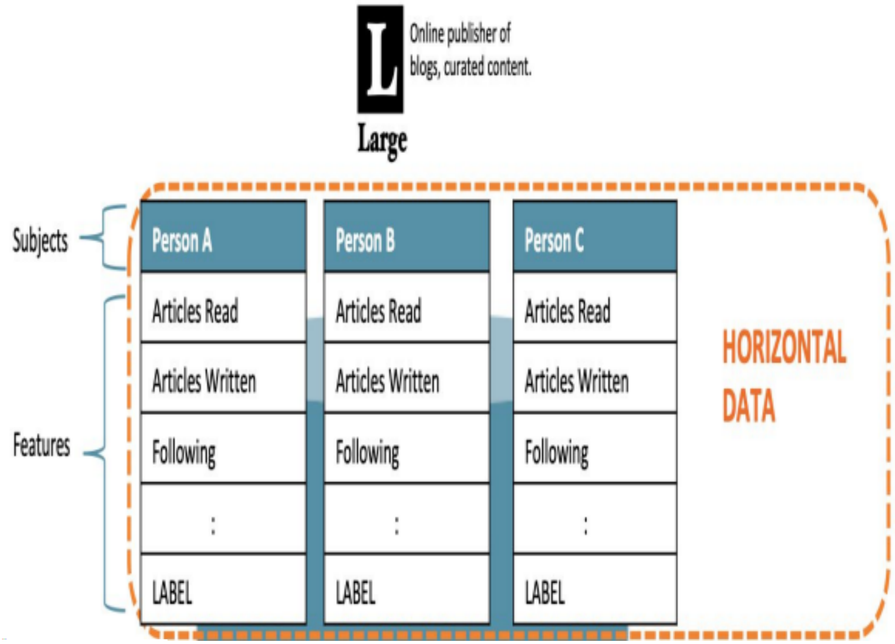
- Federated learning enables collaborative decentralized model training without sharing raw data and ensuring data privacy.

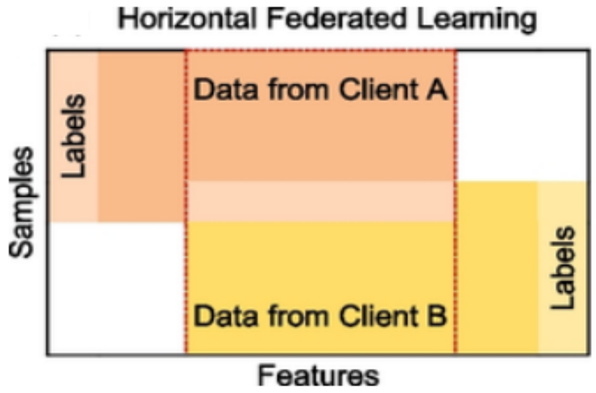
- We categorize federated learning into three main types based on data distribution:
  - Horizontal Federated Learning
  - Vertical Federated Learning
  - Federated Transfer Learning (FTL)

# Topics in Deep Learning

## Horizontal Federated Learning

- **Horizontal federated learning** uses datasets with the same feature space across all devices
- Shared features, different users: Clients have the same set of features.
- Focus is on leveraging the diversity of users with the same data structure to enhance model accuracy and generalization.
- **Example**: Multiple banks training a fraud detection model using transaction data (shared features) from different customers (different users).

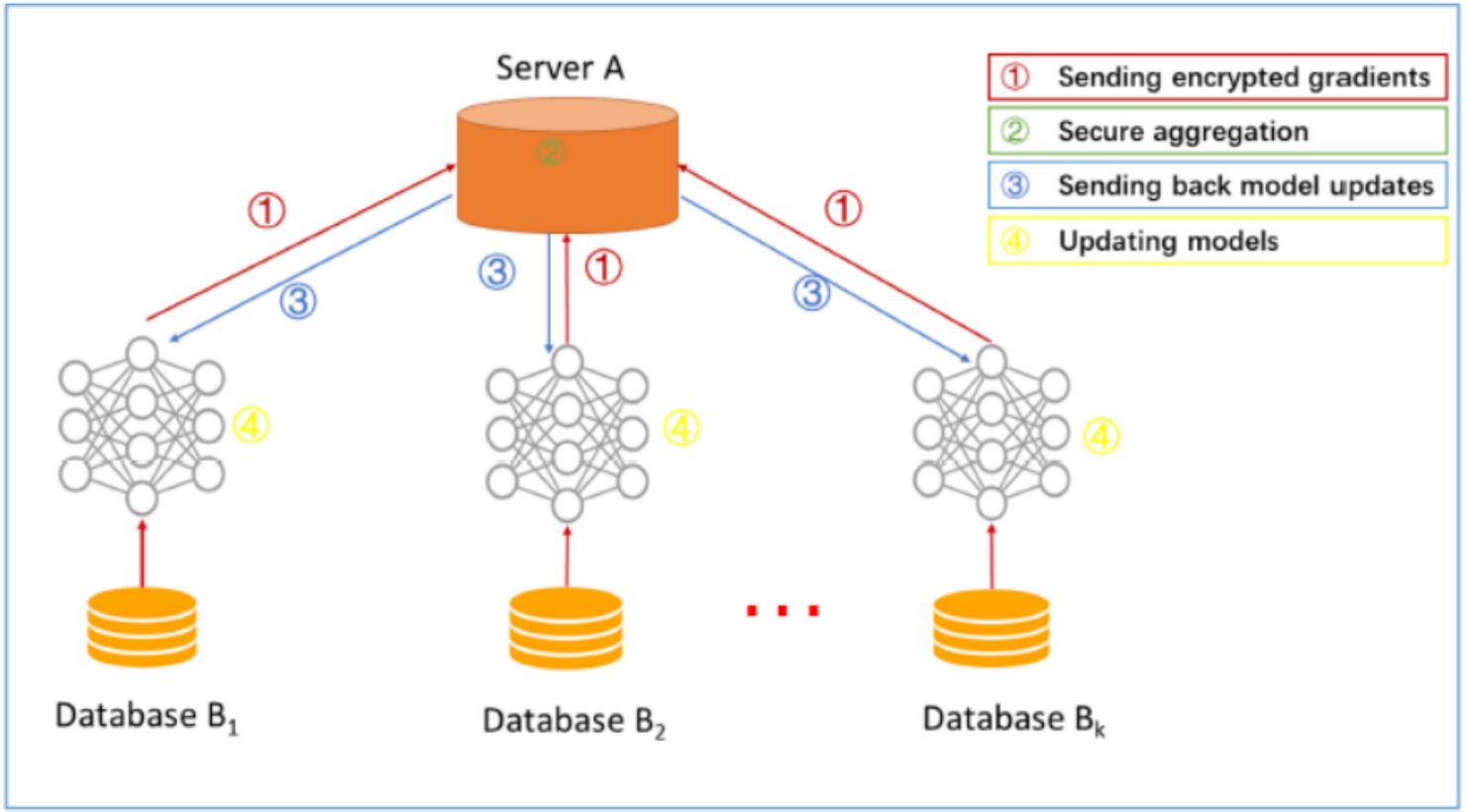



- Large overlap of features of the two data sets

# Topics in Deep Learning

## Horizontal Federated Learning

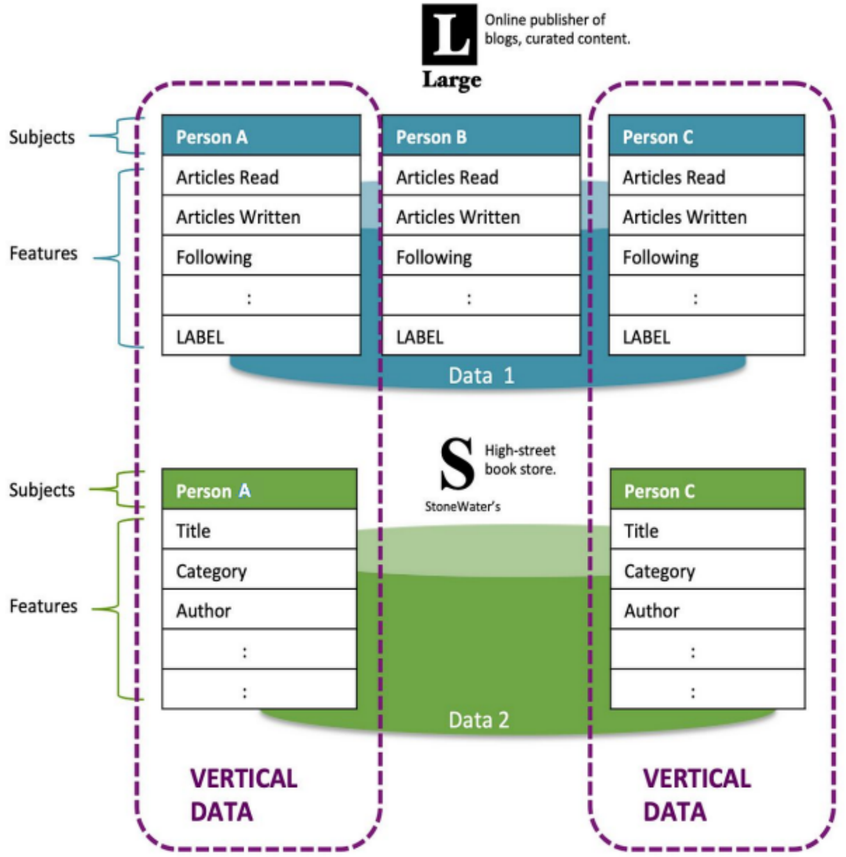


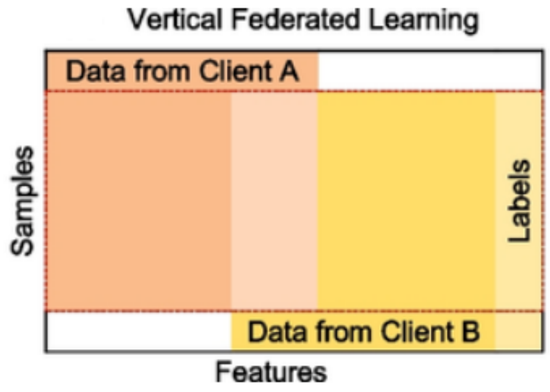

**Horizontal Federated Learning** applies to circumstances where we have a lot of overlap on features but only a few on instances. This refers to the Google Gboard use case and models can be ensembled directly from the edge models.

# Topics in Deep Learning

## Vertical Federated Learning

- **Vertical federated learning** uses different datasets of different feature space to jointly train a global model
- Different features, overlapping users: Clients have different feature sets but some features might overlap.
- Focus is on combining data from participants with complementary information while protecting sensitive features.
- **Example**: Hospitals and insurance companies collaborating on healthcare predictions using medical records (Hospital data) and policy data (Insurance data) with overlapping features like patient IDs.

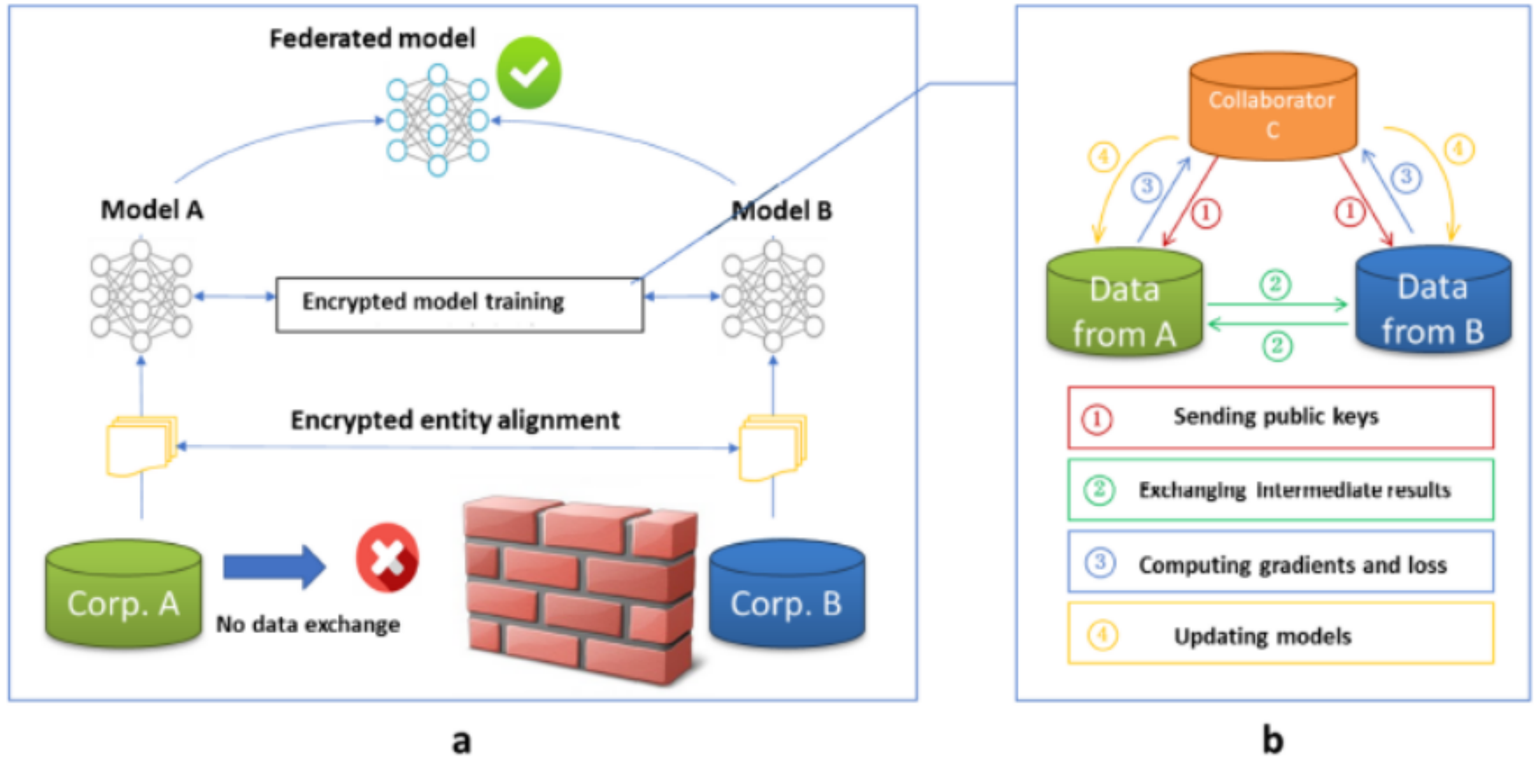



- Large overlap of sample IDs (users) of the two data sets

# Topics in Deep Learning

## Vertical Federated Learning

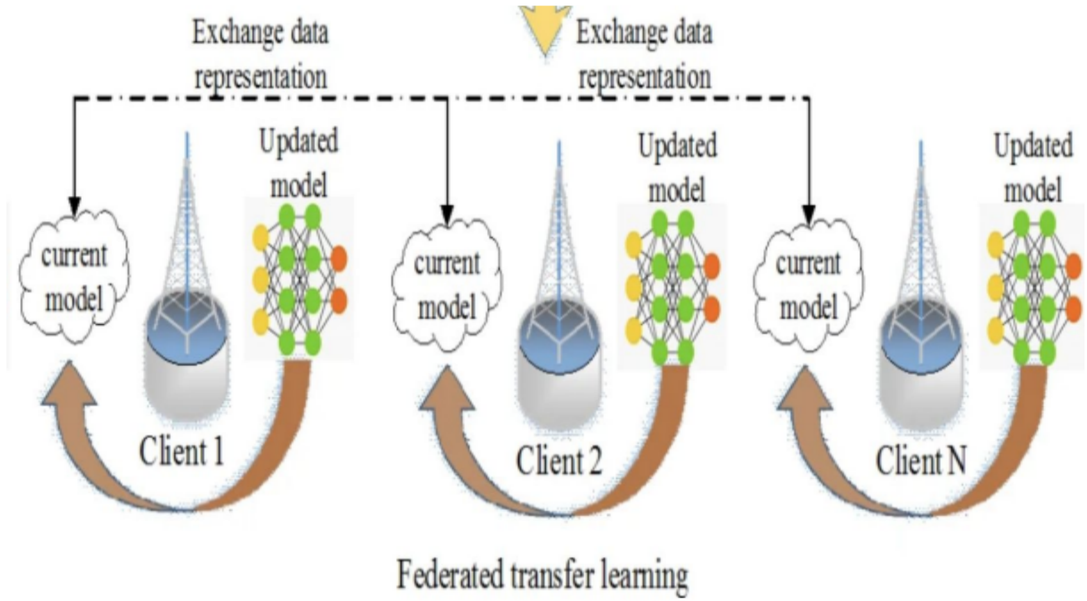



**Vertical Federated Learning** refers to where we have many overlapped instances but few overlapped features. An example is between banks and online-retailers. They both have lots of same users, but each own their own features and label data. Vertical Federated Learning merges the features together to create more powerful feature space for machine learning tasks and uses homomorphic encryption to provide protection on data privacy.

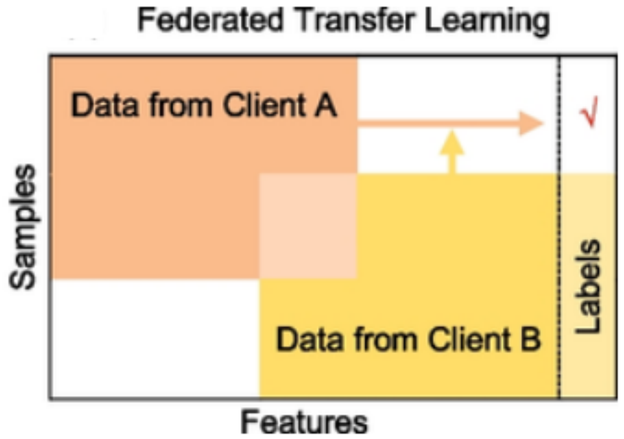
# Topics in Deep Learning

## Federated Transfer Learning (FTL)

- **Federated transfer learning** is utilized a pre-trained model for solving a different problem.
- Leveraging pre-trained knowledge: Uses a pre-trained model to guide learning on a new task or data with different characteristics.
- Focus is on accelerating learning on new tasks or data with limited resources, especially when privacy concerns restrict model sharing.
- **Example**: Using a sentiment analysis model trained on public product reviews to personalize recommendations within a specific e-commerce domain.

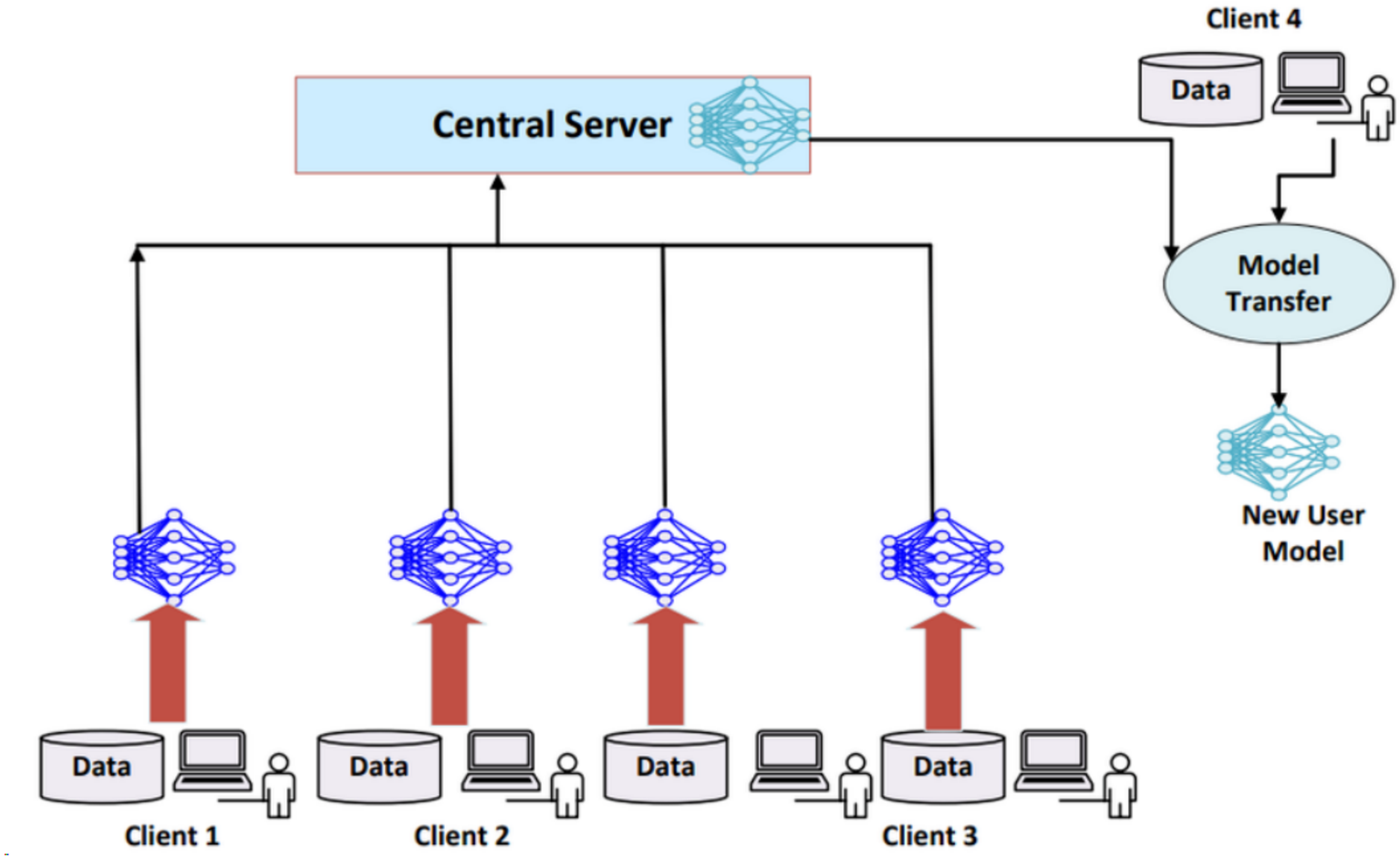


Federated transfer learning

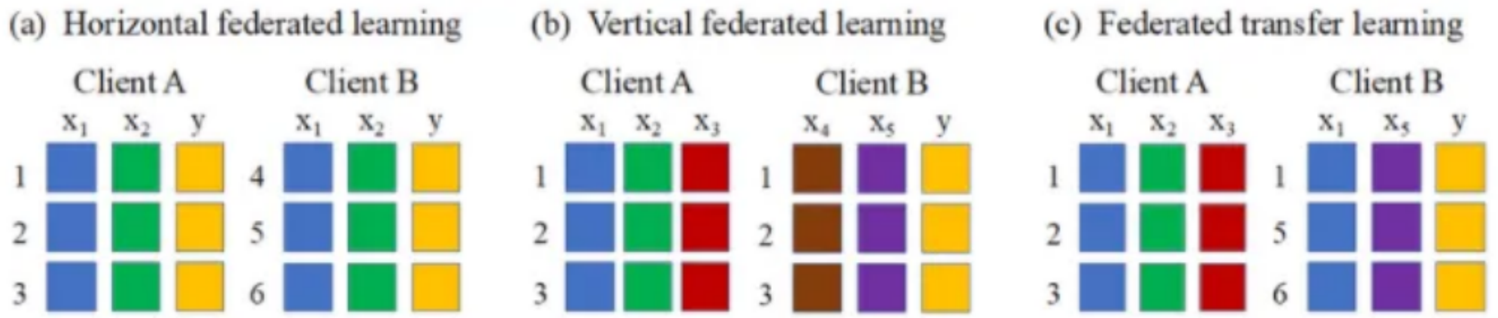


# Topics in Deep Learning

## Federated Transfer Learning (FTL)



# Conclusion




Here, 1, 2, 3, 4, 5, 6 represent the samples;
x1,x2,x3,x4,x5,x6 represent the features and y is the label

In summary,

- HFL excels in minimizing communication overhead and preserving data privacy in scenarios with diverse data instances but common features.
- VFL is effective for collaborative model training with complementary data across features while maintaining data privacy.
- FTL enables knowledge transfer and adaptation between distinct domains, enhancing model generalization and adaptation capabilities across diverse data distributions.

Each approach offers specific advantages tailored to different federated learning scenarios and objectives.

## Acknowledgements

https://towardsdatascience.com/introduction-to-federated-learning-and-challenges-ea7e02f260ca

https://www.crownpku.com/2019/03/13/A-Practical-Overview-of-Federated-Learning.html


# THANK YOU

**Dr. Shylaja S S**
Director of Cloud Computing & Big Data (CCBD), Centre for Data Sciences & Applied Machine Learning (CDSAML)
Department of Computer Science and Engineering
**shylaja.sharath@pes.edu**

**Ack: Divya K,**
**Teaching Assistant**