# COMP39/9900 Computer Science/IT Capstone Project
# School of Computer Science and Engineering, UNSW

**Project Number:** P2

**Project Title:** Privacy-Preserving Federated Learning for Medical X-Rays

**Project Clients:** Dr Basem Suleiman and Piyavachara Nacchanandana (Research Student).

**Number of groups:** 2

**Main contact:** Piyavachara Nacchanandana

**Project Specializations:** Artificial Intelligence (Machine/Deep Learning, NLP);Bioinformatics/Biomedical

**Background:** The increasing amount of sensitive data generated and stored across various devices and organizations has raised significant privacy concerns. Traditional centralized machine learning approaches, where data is collected in a central location, pose risks of data breaches and misuse. Federated learning (FL) has emerged as a promising solution to address these challenges by enabling collaborative model training without directly sharing raw data.

**Project Goals:**

*Privacy Preservation*: The primary goal is to design and implement a federated learning system that prioritizes privacy by ensuring that sensitive data remains decentralized and is not directly shared with a central server or other clients.

*Model Performance*: The project aims to achieve comparable or even superior model performance to centralized machine learning approaches, demonstrating the effectiveness of federated learning in real-world scenarios.

*Application-Specific Optimization*: Tailor the federated learning system to the specific application domain, optimizing it for the unique characteristics and challenges of the chosen field (e.g., healthcare, finance, IoT).

*Evaluation and Comparison*: Rigorously evaluate the performance of the FL system in terms of accuracy, privacy preservation, communication efficiency, and scalability. Compare it with traditional centralized approaches to highlight the advantages and limitations.

*Real-World Impact*: Contribute to the growing body of knowledge in federated learning and its potential to revolutionize privacy-preserving machine learning applications.

**Requirements and Scope:**

*Federated Learning Architecture*: Design and implement a federated learning architecture tailored to the chosen application domain. This includes defining the roles of clients and servers, data partitioning strategies, model aggregation algorithms, and communication protocols.

*Privacy-Preserving Techniques*: Integrate privacy-preserving techniques into the FL system, such as differential privacy, secure aggregation, or homomorphic encryption, to protect sensitive data during the training process.

*Data Preprocessing and Feature Engineering*: Explore appropriate data preprocessing and feature engineering methods to address data heterogeneity and ensure the quality and relevance of features used in the FL model.

*Model Selection and Optimization*: Investigate different machine learning models suitable for federated learning and optimize hyperparameters to achieve the best possible performance.

*Experimental Evaluation*: Conduct comprehensive experiments to evaluate the performance of the FL system on real-world datasets or simulated data representative of the chosen application domain.

**Out of Scope:**

*Hardware Implementation*: The project will focus on the software implementation of the FL system, not hardware acceleration or optimization.

*Deployment in Production Environments*: While the project will create a working prototype, deploying it in a production environment is beyond the scope of this capstone.

*Data*: Identify suitable datasets for the chosen application domain that are representative of real-world scenarios. If real-world data is not available or accessible, generate synthetic data that mimics the characteristics of the target domain. Define a clear data partitioning strategy (e.g., by user, by organization) for the federated learning process.

*Architecture*: Design the overall architecture of the FL system, including the roles and responsibilities of clients and the server. Specify the communication protocols and mechanisms for model updates and aggregation. Determine the frequency of communication between clients and the server.

*Privacy*: Choose and implement appropriate privacy-preserving techniques (e.g., differential privacy, secure aggregation) to protect sensitive data.
Quantify the privacy guarantees of the chosen techniques using relevant metrics.
*Evaluation*: Define evaluation metrics for the project, including model accuracy, privacy preservation, communication efficiency, and scalability. Develop a

comprehensive evaluation plan to assess the performance of the FL system against these metrics. Compare the results with traditional centralized machine learning approaches.

**Required Knowledge and skills:**

Machine Learning Fundamentals: Strong understanding of machine learning concepts, algorithms (e.g., regression, classification, neural networks), and evaluation metrics.

Federated Learning: Knowledge of federated learning principles, architectures, and challenges.

Programming: Proficiency in Python and experience with machine learning libraries (e.g., TensorFlow, PyTorch) and federated learning frameworks (e.g., TensorFlow Federated).

Privacy and Security: Understanding of privacy-preserving techniques (e.g., differential privacy, secure aggregation) and security considerations in distributed systems.

Data Processing: Familiarity with data preprocessing, feature engineering, and handling data heterogeneity.

Problem-Solving: Ability to analyze complex problems, design solutions, and implement them effectively.

**Expected outcomes/deliverables:**

A working federated learning system tailored to the chosen application domain.

Thorough evaluation of the system's performance and privacy guarantees.

A comprehensive report detailing the project's findings, challenges, and potential future direction.

**Supervision:**

Piyavachara Nacchanandana

**Additional resources:**

TBC