**Cover Page of the Dissertation**

Federated Learning with Context-Aware Model Orchestration and Privacy Preservation Using Differential Privacy

DISSERTATION

Submitted in partial fulfillment of the requirements of the

Degree: MTech in Data Science and Engineering

By

Sourav Bhattacharjee

2023DA04045

Under the supervision of

Pradeep Rai

Senior Manager, Risk Management

BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE

Pilani (Rajasthan) INDIA

July, 2025

### Table of Contents

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Description** | **Page Number** |
| 1. | Dissertation Abstract | 3-7 |
| 2. | EDA of Dataset (CIFAR 10) |  |
| 3. | List of Symbols & Abbreviations used |  |
| 4. | List of Tables |  |
| 5. | List of Figures |  |
| 6. | Chapter 1 |  |
|  | Chapter 2 |  |
|  | Chapter 3 |  |
|  | Directions for future work after mid semester |  |
|  | Summary of the literature survey |  |
| 11. | Bibliography / References |  |

**1. Dissertation Outline (Abstract)**

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**SECOND SEMESTER 2024-25**

DSECLZG628T **DISSERTATION**

Dissertation Title : Federated Learning with Context-Aware Model Orchestration and Privacy Preservation Using Differential Privacy

Name of Supervisor : Pradeep Rai

Name of Student : Sourav Bhattacharjee

ID No. of Student : 2023DA04045

Courses Relevant for the Project & Corresponding Semester:

| **Semester** | **Course No.** | **Course Title** | **Justification** |
| --- | --- | --- | --- |
| 1 | DSECL ZG532 | Introduction to Data Science | Provided fundamentals of data handling and ML workflows. |
| 2 | DSECL ZG565 | Machine Learning | Core concepts for model training and evaluation in FL. |
| 2 | DSECL ZG529 | Data Management for Machine Learning | Helped simulate distributed clients and data flows. |
| 3 | DSECL ZG524 | Deep Learning | Enabled design of CNN models used in clients. |

## Abstract

Clearly specify somewhere that the objective is not accuracy, but to show that the overall system works. This is more of building a system. Accuracy can be improved by using large CNNs on GPUs. Also specify somewhere, that model bigcnn and smallcnn have the same architectures. Give reason for this. And why this is needed. Give updated drawings also.

**Key Words:** Federated Learning, Model Context Protocol, Differential Privacy, Decentralized AI, Privacy-Preserving Machine Learning, Flower, Adaptive AI Models

The increasing deployment of machine learning models across edge devices and distributed systems has introduced critical challenges related to **device heterogeneity**, **data privacy**, and **computational efficiency**. Devices participating in real-world machine learning tasks often differ in processing power, memory, and network connectivity. At the same time, data generated on such devices is often sensitive—especially in domains like healthcare and finance—making centralized model training infeasible due to regulatory and ethical concerns. This dissertation proposes a novel federated learning framework that addresses these issues through the integration of **Model Context Protocol (MCP)** and **Differential Privacy (DP)** mechanisms.

The system is designed to support federated learning (FL), where multiple clients collaboratively train a global model without sharing raw data. Instead of transmitting private datasets, each client performs local training on its own data and shares only the model weight updates with a central server, which aggregates them into a global model. A key feature of this system is its support for **user-driven model selection** via command-line prompts. At the time of launch, each client explicitly selects between a lightweight (SmallCNN) or heavyweight (BigCNN) model, allowing users to tailor the model choice to their device’s computational capacity.

To ensure **data privacy**, each client incorporates **differential privacy techniques** during local training. Using the Opacus library, noise is added to gradients or model parameters before they are shared with the server, thereby limiting the possibility of reconstructing any individual’s data from the model updates.

The system is developed using the **Flower federated learning framework**, and validated using the **CIFAR-10 dataset**, which is distributed across clients in a non-IID fashion to simulate real-world variations in data availability and quality. Clients autonomously measure their system context through local monitoring tools and select the appropriate model accordingly. Local training is performed under privacy-preserving constraints, and the federated server performs secure aggregation of the received model updates to improve a shared global model iteratively over multiple training rounds.

The project demonstrates how the combination of **federated learning**, **context-aware model orchestration**, and **differential privacy** can yield a flexible, adaptive, and secure machine learning system. This approach has practical relevance to scenarios where **data sensitivity and device variability** are both dominant concerns, such as in mobile health applications, smart home ecosystems, and financial transaction analysis. The proposed framework is designed to be modular and extensible, making it suitable for future enhancements like real-time personalization and on-device inference optimization.

Overall, this work presents a comprehensive solution to contemporary challenges in decentralized AI, offering both theoretical robustness and implementation feasibility.

Why have the model choice been made explicit at runtime:

**Advantages of Explicit Model Selection**

**1. User Awareness and Control**

* **Reason**: Some users or developers may want full control over which model is used, especially in experimental or testing scenarios.
* **Advantage**: Enables deliberate testing of model performance under different hardware conditions or datasets.

**2. Simplified Debugging and Reproducibility**

* **Reason**: Knowing exactly which model was used on each client simplifies tracking bugs or anomalies.
* **Advantage**: Makes experiments deterministic and results reproducible, which is critical for academic research and benchmarking.

**3. Avoids Unintended Overhead**

* **Reason**: Context-aware dynamic switching requires continuous system monitoring and decision logic (CPU, memory checks).
* **Advantage**: Removing this complexity reduces runtime overhead, making the system lighter and easier to deploy in constrained environments.

**4. Works on All Systems (Including Headless/Cloud Clients)**

* **Reason**: Some client systems (like edge devices or cloud VMs) may not expose real-time hardware metrics.
* **Advantage**: Explicit input works universally across all environments without hardware-level integration.

**5. Better for Education and Demonstration**

* **Reason**: When teaching federated learning concepts, it helps to isolate model-related decisions from system context.
* **Advantage**: Makes it easier to demonstrate the impact of model complexity on training time, accuracy, and communication cost.

**6. Fine-Grained Testing of Model Performance**

* **Reason**: Developers may want to test how SmallCNN and BigCNN individually contribute to global performance.
* **Advantage**: Enables scenario-based testing like “What happens if 3 out of 5 clients use BigCNN?”

**7. Avoids Inaccurate or Inconsistent Context Detection**

* **Reason**: CPU/memory usage may not accurately reflect resource availability, especially on shared or virtualized systems.
* **Advantage**: Manual selection avoids false triggers or suboptimal auto-choices made under misleading system states.

### Context-Aware Model Assignment for Real-World Mobile Apps

In a real-world mobile application that trains models based on user interactions, devices vary greatly in hardware capabilities. To ensure optimal performance across this diversity, our system assigns model architectures dynamically based on each device’s specs.

For example, lower-end phones receive a lightweight model (SmallCNN), while high-performance devices are assigned a larger model (BigCNN). This assignment is made at runtime by checking CPU capacity, memory, and other system metrics.

This approach ensures:

* **Smooth app performance** across all devices
* **Inclusive participation** in federated learning
* **Efficient use of resources**, preserving battery and responsiveness
* **Balanced global training**, leveraging both simple and complex models

By adapting models to the device, the system delivers intelligent personalization without compromising user experience or system stability.

**BIRLA INSTITUTE OF TECHNOLOGY AND SCIENCE, PILANI**

**II SEMESTER 24-25**

DSECLZG628T **DISSERTATION**

**Dissertation Outline (Abstract)**

**BITS ID No.:** 2023DA04045

**Name of Student:** Sourav Bhattacharjee

**Name of Supervisor:** Pradeep Rai

**Designation of Supervisor**: Senior Manager – Risk Management

**Qualification and Experience:** M.S in Business Analytics

16 years of experience in risk management using analytics

**Official E- mail ID of Supervisor:** pradeep1930delhi@gmail.com

**Topic of Dissertation**: Federated Learning with Context-Aware Model Orchestration and Privacy Preservation Using Differential Privacy

A close-up of a black letter

Description automatically generated

A close-up of a text

Description automatically generated

(Signature of Student) (Signature of Supervisor)

Date: 22nd May 2025 Date: 22nd May 2025

### Broad Area of Work

Machine Learning, Privacy-Preserving AI, Distributed Systems

### Objectives

The objectives of my project are as follows:

* To design and implement a federated learning (FL) system in which each client selects between lightweight and heavyweight model architectures explicitly using command-line input, simulating resource-aware deployment decisions. The system supports model flexibility through a Model Context Protocol (MCP) interface, which enables this explicit selection per client.

*Methodology*: Each client was designed to **explicitly select between a lightweight (SmallCNN) or a heavyweight (BigCNN) model** using a command-line argument at runtime. This explicit selection approach allows users or deployment scripts to choose the model architecture best suited for a given device’s computational capacity or operational context.

The federated learning process was orchestrated using the **Flower framework**, enabling decentralized model training. Clients performed local training on private data using the selected model and sent only the model weight updates to the central server. The server aggregated these updates to build a shared global model without accessing raw client data.

This setup ensures modularity, reproducibility, and user control, making it practical for environments where resource conditions are known ahead of time or dictated by deployment policies.

* To implement **two distinct convolutional neural network** (CNN) architectures—a **deep CNN** serving as the heavyweight model for high-performance training, and a **lightweight CNN** optimized for resource-constrained scenarios—both designed to maintain comparable predictive capabilities on the CIFAR10 dataset

*Methodology*: The **heavyweight model** consists of multiple convolutional and dense layers (e.g., 3–4 Conv2D layers + 2 Dense layers), while the **lightweight model** uses a simplified structure (e.g., 1–2 Conv2D layers + 1 Dense layer). Both models are trained and evaluated independently, then integrated into the Flower client with dynamic selection logic based on system CPU load. The CNN architectures are kept simple, as the main focus is the demonstration of Federated Learning.

* **To integrate Differential Privacy (DP) into local training** using the Opacus library, and to validate its effectiveness through Membership Inference Attack (MIA) simulations based on the methodology of Shokri et al. (2017). The system should demonstrate that DP reduces privacy leakage while maintaining model performance.

*Methodology*: Achieve a final privacy budget of **ε ≤ 4.0**, with **Membership Inference Advantage ≤ 0.05** under DP, and model accuracy loss limited to **≤ 10%** compared to the non-private baseline.

* **To monitor and log model switching behaviour and system resource metrics** (such as CPU usage and memory load) in real time, providing transparency and traceability of client decision-making.

*Methodology*: Real-time logs should capture **100% of model switches.**

Integrate the entire system

Methodology

### Scope of Work

The scope of this dissertation is to design, develop, and validate a fully functional AI system that integrates three key components: Federated Learning (FL), Model Context Protocol (MCP) for adaptive model selection based on system resources, and Differential Privacy (DP) for secure local training. The system will be built using open-source tools including PyTorch, Opacus, and Flower, and will be evaluated using the CIFAR-10 dataset. Validation will include both performance metrics (accuracy, resource usage) and privacy benchmarks (epsilon budget and Membership Inference Advantage), ensuring the solution is scalable, interpretable, and grounded in current research practices.

### Detailed Plan of Work (16 Weeks)

| **S. No.** | **Task/Phase Description** | **Start–End Dates** | **Duration (weeks)** | **Deliverables** |
| --- | --- | --- | --- | --- |
| 1 | Literature Review (FL, DP, MCP), Dataset setup | Week 1–2 | 2 | Research summary, CIFAR-10 client splits |
| 2 | Basic model training (SmallCNN & BigCNN) | Week 3–4 | 2 | Trained baseline models |
| 3 | Set up Flower FL system (server + clients) | Week 5–6 | 2 | Working FL loop with static model |
| 4 | Enable explicit model selection (SmallCNN/BigCNN) via command-line input for clients | Week 7 | 1 | Model Context Protocol working |
| 5 | Integrate differential privacy using Opacus | Week 8–9 | 2 | DP-enabled client training |
| 6 | Full FL system integration (MCP + DP + FL) | Week 10-11 | 2 | End-to-end system ready |
| 7 | Run experiments: model switching vs context | Week 12–13 | 2 | Experiment results |
| 8 | Documentation: report writing and result analysis | Week 14–15 | 2 | Draft dissertation |
| 9 | Finalization, viva prep, PPT, demo recording | Week 16 | 1 | Final report + presentation |

### Literature References

The following are referred journals from the preliminary literature review.

1. Federated learning with differential privacy for breast cancer diagnosis enabling secure data sharing and model integrity - <https://www.nature.com/articles/s41598-025-95858-2>

2. Differentially Private Federated Learning: A Systematic Review - <https://arxiv.org/abs/2405.08299>

3. A Systematic Survey for Differential Privacy Techniques in Federated Learning - <https://www.scirp.org/journal/paperinformation?paperid=123374>

4. Membership Inference Attacks Against Machine Learning Models –

<https://arxiv.org/abs/1610.05820>

**Supervisor’s Rating of the Technical Quality of this Dissertation Outline**

EXCELLENT / GOOD / FAIR/ POOR (Please specify): EXCELLENT

**Supervisor’s suggestions and remarks about the outline (if applicable).**

A close-up of a black letter

Description automatically generated

Date: 22nd May 2025 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Signature of Supervisor)

Name of the supervisor: Pradeep Rai

Email Id of Supervisor: pradeep1930delhi@gmail.com

Mob # of supervisor: 8800896370

**2. EDA of Dataset (CIFAR 10)**

The CIFAR-10 dataset is used in this project to simulate federated learning environments across clients. It comprises 60,000 colour images of 32×32 pixels across 10 distinct classes, equally split between training and test sets.

**Dataset Overview**

* **Classes**: airplane, automobile, bird, cat, deer, dog, frog, horse, ship, truck
* **Training samples**: 50,000
* **Test samples**: 10,000
* **Image shape**: 3 channels (RGB) × 32 × 32 pixels
* **Data balance**: Uniform across all classes

### Sample Images per Class

One representative image from each class was displayed using matplotlib. This allowed a quick visual inspection to confirm the semantic diversity of the dataset.

* Images like “automobile” and “truck” show visual similarity.
* Others like “frog” or “ship” are distinct and easily separable.

Insert here

*Purpose*: Helps validate the class mapping and assess visual variability.

### Class Distribution

A bar plot of label counts shows a perfectly **balanced dataset**, with **6,000 images per class**.

Insert here

*Why this matters*: No resampling or weighting strategies are needed during model training.

### Average Image per Class

The mean image was computed for each class by averaging pixel values across all training images in that class.

* Structured objects (e.g., *airplane*, *automobile*) retained more visible shapes in average images.
* Natural or deformable objects (e.g., *cat*, *dog*) appeared blurrier, reflecting high intra-class variance.

*Inference*: Average images offer insight into the variance and sharpness of features per class, which influence classification difficulty.

Insert here

### Color Channel Correlation Matrix

All pixel values were flattened, and the Pearson correlation coefficient was calculated between R, G, and B channels.

Insert here

*Interpretation*: Strong correlation between red and green is typical in natural images.

### Key Reasons for Choosing CIFAR-10:

1. **Open Source & Publicly Available**

Due to organizational constraints at American Express and ethical compliance requirements, proprietary or sensitive data could not be used in academic research. CIFAR-10, being a well-established open-source dataset, ensures legal and reproducible experimentation without any privacy or usage restrictions.

1. **Federated Learning Compatibility**

CIFAR-10’s structure and size make it ideal for **simulating federated learning environments**, where the dataset can be artificially partitioned into non-IID subsets to mimic real-world client variability. This allows for realistic testing of federated aggregation and local training.

1. **Visual Complexity & Diversity**

The dataset contains 60,000 32×32 RGB images across 10 balanced classes. The images span various categories (animals, vehicles, etc.), introducing enough **inter-class and intra-class variability** to effectively evaluate model robustness, switching logic (based on system load), and generalization under resource constraints.

1. **Well-Studied Benchmark**

CIFAR-10 is a widely used benchmark in both academia and industry for evaluating **convolutional neural networks, privacy mechanisms**, and **distributed learning setups**. Its use facilitates comparisons with established baselines and ensures the validity of empirical results.

1. **Lightweight for Resource-Constrained Testing**

The small image size (32×32 pixels) and manageable dataset size make CIFAR-10 **computationally feasible to run on a single machine**, such as a MacBook, especially under stress simulation conditions. This aligns well with the MCP (Model Context Protocol) objective of adapting to CPU/memory load dynamically.

1. **Support for Differential Privacy Analysis**

CIFAR-10’s moderate complexity enables the application of **differential privacy** via noise injection during local training while still allowing measurable drops in performance, which is critical for visualizing the privacy-utility trade-off. It also supports **Membership Inference Attacks (MIA)** for validating that DP is working effectively.

**Chapter 1: Objectives and Midterm Status**

**🔹 Objective 1: Set up Flower FL system and integrate logic for model context switching using psutil and ngstress**

**Objective:** To setup a federated learning (FL) system locally in which each client dynamically selects between lightweight and heavyweight CNN architectures based on real-time system resource usage, using a Model Context Protocol (MCP).

**Midterm Status: ✅ Completed**

* The **Model Context Protocol (MCP)** was implemented in flower\_client.py. It monitors CPU usage using psutil.
* Clients switch to the **lightweight model** (SmallCNN) when CPU availability > 60%, and back to **heavyweight model** (BigCNN) when usage < 60%.
* The FL setup uses **Flower** for client-server orchestration.
* Stress testing using **ngstress** was integrated to validate the model-switching logic under artificial CPU load.

**🔹 Objective 2: Implementation of Lightweight and Heavyweight CNNs**

**Objective:** To implement two distinct CNNs—a deep CNN (heavyweight) for high performance and a small CNN (lightweight) for constrained devices, both optimized for CIFAR-10.

**Midterm Status: ✅ Completed**

* Defined in models.py:
  + SmallCNN: 1 Conv layer + MaxPool + 1 Dense layer.
  + BigCNN: 2 Conv layers + MaxPool + 2 Dense layers.
* Both models tested independently to ensure baseline accuracy on CIFAR-10.
* Integrated into the Flower client with dynamic switching logic.

**🔹 Objective 3: Implementation of Differential Privacy proof-of-concept and integration into the overall system**

**Objective:** To integrate Differential Privacy (DP) in local training using **Opacus**, and validate effectiveness via Membership Inference Attack (MIA) simulations.

**Midterm Status: 🟡 In Progress**

* Integrated Opacus via privacy\_wrapper.py:
  + PrivacyEngine is applied to local training within the Flower client.
  + Per-round ε (epsilon) is logged.
* A separate proof-of-concept (dp\_proof\_demo.py, dp\_streamlit\_demo.py) validates MIA resistance.
* Ongoing work:
  + Run end-to-end simulations to evaluate final ε ≤ 4.
  + Assess model accuracy drop and MIA advantage as per Shokri et al. (2017).

**🔹 Objective 4: Real-time Logging of Model Switching and System Metrics**

**Objective:** To monitor and log model switching behavior and system metrics (CPU usage, memory) in real time.

**Midterm Status: ✅ Completed**

* Implemented in utils.py and flower\_client.py:
  + CPU usage is sampled every 5 seconds.
  + All model switches (Small ↔ Big) are logged to timestamped logs.
* Real-time visualization included in dashboard\_app.py (Streamlit-based).

**Chapter 2: Set up Flower FL system and integrate logic for model context switching using psutil and ngstress**

**Chapter 3: Implementation of Lightweight and Heavyweight CNNs**

A diagram of a company

Description automatically generated

Small CNN Implemented

**A diagram of a company

Description automatically generated**

Big CNN Implemented

**Chapter 4: Implementation of Differential Privacy proof-of-concept and integration into the overall system**

**3. Directions for future work after mid semester**

**4. Summary of the literature survey**

**1. Federated Learning with Differential Privacy for Breast Cancer Diagnosis Enabling Secure Data Sharing and Model Integrity**

**Link**: [Nature, 2025](https://www.nature.com/articles/s41598-025-95858-2)

I referred to this paper as it shows how **federated learning (FL)** can be used in a sensitive domain like healthcare, where data privacy is critical. The authors combine FL with **differential privacy (DP)** to ensure patient data never leaves local devices, and model updates are privacy-protected. This aligned closely with my goal of creating a privacy-preserving FL setup that works across resource-constrained or privacy-sensitive clients, similar to the environment I aim to simulate in my work.

### 2. Differentially Private Federated Learning: A Systematic Review

**Link**: [arXiv, 2024](https://arxiv.org/abs/2405.08299)

This paper helped me understand the different strategies used to apply **differential privacy in federated systems**, including where and how to inject noise, how to manage clipping, and the tradeoff between privacy and accuracy. I used this review to justify my decision to use **Opacus**, which performs per-sample gradient clipping and Gaussian noise injection. The review also emphasized transparency and interpretability, which I have implemented through attack simulations and detailed metrics to show that my system is not a black box.

### 3. A Systematic Survey for Differential Privacy Techniques in Federated Learning

**Link**: [SCIRP, 2023](https://www.scirp.org/journal/paperinformation?paperid=123374)

This survey deepened my understanding of how different DP mechanisms (Laplace, Gaussian, etc.) perform under federated setups. It was especially useful when benchmarking my own model’s performance in terms of **privacy budget (ε)** and **accuracy drop**. The paper emphasized the importance of maintaining an acceptable accuracy threshold while preserving privacy, which became one of the core goals in my implementation and evaluation.

### 4. Membership Inference Attacks Against Machine Learning Models

**Link**: [arXiv, 2016](https://arxiv.org/abs/1610.05820)

This foundational paper on **membership inference attacks (MIAs)** inspired my approach to **validating whether differential privacy is truly effective**. The concept of MI Advantage — measuring the difference in model confidence for seen vs unseen data — became a central part of my project. I recreated this attack to quantify and demonstrate how privacy leakage is reduced when DP is applied, and this gave me strong, reproducible evidence that privacy is being enforced in my system.

Github Code link:

<https://github.com/srv48/mcp_federated_diff_privacy.git>