I. Format of the 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

May, 2025

II. The following format for Dissertation Outline (Abstract) should be used

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

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. Each client instead trains a local model using its own dataset and contributes only model updates to a central aggregation server. The novelty of this work lies in its incorporation of **dynamic model selection** using a **Model Context Protocol**, which enables clients to select between lightweight and heavyweight model architectures based on their **real-time resource conditions**, such as CPU and memory usage. This allows the system to efficiently adapt to the computational limitations of diverse devices without compromising their ability to contribute to training.

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.

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

Sourav Bhattacharjee

P. Rai

(Signature of Student)

(Signature of Supervisor)

Date: 22nd May 2025

Date: 22nd May 2025

1. Broad Area of Work

Machine Learning, Privacy-Preserving AI, Distributed Systems

2. Objectives

The objectives of my project are as follows:

- To build a federated learning system where clients adaptively select models based on system resource availability.
- To preserve data privacy through differential privacy during local training.
- To monitor model switching behaviour and system context in real time.

3. Scope of Work

Scope of this dissertation is to design and develop a fully functional AI system that combines federated learning, model context adaptation, and differential privacy. The system will be implemented using open-source tools and validated using a standard dataset.

4. 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	Implement context engine (CPU/memory detection) and dynamic model switching	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

S. No.	Task/Phase Description	Start–End Dates	Duration (weeks)	Deliverables
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

5. 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

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).

Date: 22nd May 2025

P. Rai

(Signature of Supervisor)

Name of the supervisor: Pradeep Rai

Email Id of Supervisor: pradeep1930delhi@gmail.com

Mob # of supervisor: 8800896370