Indian Institute of Technology Kanpur
Department of Computer Science and Engineering
Proposal for a New Course

1. **Course Title**: **Differential Privacy in Machine Learning**
2. **Course No**.:
3. **Credits**: 3-0-0-0 [9].
4. **Duration of Course**: Full Semester
5. **Who can take this course**: Any UG student who has done CS203 (or, equivalent) or CS771 (or. equivalent) and any PG student is eligible for doing this course. Instructor's consent will be needed for enrolling in this course. Moreover, while deciding enrolment some filtering may be used based on the performance in the courses (Desirable: at least A grade in CS203 or at least B grade in CS771).
6. **Proposing Department**: CSE
7. **Other Departments/IDPs which may be interested in the proposed course**: Mathematics, Electrical Engineering.
8. **Other faculty members interested in teaching the proposed course**: Any faculty member from the area of information theory and machine learning.
9. **Proposing Instructor**: Sayak Ray Chowdhury, Department of CSE.
10. **Objectives**: How can we extract insights from a dataset containing sensitive information while ensuring the privacy of the individuals it includes? This course addresses this question by examining the limitations of simple approaches and advancing to solutions involving differential privacy. The class will cover fundamental principles of differential privacy, delve into algorithms for attaining privacy, and explore applications in statistics and machine learning. Students will complete mathematical exercises, engage in programming tasks, and undertake a final project as part of the course (in groups; depending on the size of the batch).
11. **Contents**:

S.No	Broad Title	Topics	No. of Lectures
1.	Overview and Motivation of the course	Course logistics and evaluation details	1
2.	Attacks on statistical data privacy	Reconstruction attacks	1

3.	What do we mean by privacy in Machine Learning?	Introduction to differential privacy Differential privacy in US Census	2
4.	Definition of Differential Privacy	Pure, approximate, concentrated and Renyi differential privacy	2
5.	Properties of Differential Privacy	Post-processing, basic and advanced composition, privacy conversions	2
6.	Algorithms for achieving Differential Privacy	Laplace mechanism, Exponential mechanism, Gaussian mechanism. Sparse vector technique, Binary tree mechanism	5
7.	Differential Privacy in Statistics	Private mean estimation Adaptive data analysis	2
8.	Differential Privacy in Machine Learning	Private empirical risk minimization Private gradient descend and moment accountants Private FTRL	5
9.	Other topics	Privacy in Game theory and mechanism Design Privacy in Online learning and multi-armed bandits Private Synthetic data generation	4
10	Project Presentations	Survey multiple papers and present a report Comparison study of private ML algorithms Open ended research projects	4

Reference books: None. However, the relevant materials will be provided

Text books / monographs:

1. The Algorithmic Foundations of Differential privacy. Cytnthia Dwork and Adam Smith.
2. The Complexity of Differential privacy. Salil P. Vadhan

Dated: 26-09-2024_____Proposer: Sayak Ray Chowdhury

Dated: 26-09-2024_____DPGC Convener: Prof. Piyush Rai

The course is approved/not-approved

SPGC/SUGC Chairperson
Dated: _____