ADVANCED ARTIFICIAL INTELLIGENCE (21AD307T)

DIFFERENTIAL PRIVACY TECHNIQUES

MITHUN RAJ S

113222072056

ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

'B' – SECTION

Objective / Scope (2)	Plan of Execution (2)	Implementation (2)	Presentation (2)	Insight on project area (2)	Total (10)

MODULE DETAILS

- Objective & Scope
- Problem Statement
- Plan of Execution
- Module 1
- Implementation
- Insight on Project Area
- Conclusion

OBJECTIVE & SCOPE

Objectives:

To design and implement differential privacy mechanisms in machine learning models, ensuring secure and privacy-preserving data handling while maintaining model accuracy.

Scope:

The project focuses on implementing differential privacy mechanisms to protect sensitive data in machine learning models. It will use noise addition techniques and privacy budgets to balance privacy and model accuracy. The implementation ensures compliance with privacy regulations like GDPR and CCPA. Finally, the system will validate privacy guarantees while maintaining model performance.

PROBLEM STATEMENT

As data privacy concerns grow, traditional machine learning models often risk exposing sensitive information, potentially violating privacy regulations. There is a need for techniques that protect individual data while maintaining the utility of the model. Differential privacy provides a solution by adding noise to data or model outputs, ensuring privacy without significantly affecting the model's accuracy. This project aims to implement differential privacy techniques to safeguard sensitive information in machine learning models, ensuring compliance with privacy regulations.

MODULE 1

- **Module 1: Preprocessing and Privacy Design - Key Components**
- **Define Privacy Requirements**: Set privacy levels (epsilon, delta).
- **Select Differential Privacy Mechanisms**: Choose noise addition methods (Laplace, Gaussian).
- **Data Preprocessing**: Anonymize, normalize, and clean the data.
- **Set Privacy Budget**: Determine the balance between privacy and accuracy.
- **Initial Testing**: Evaluate the impact of privacy mechanisms on model performance.

IMPLEMENTATION

- **Define Privacy Requirements**
  Set the privacy parameters (epsilon and delta) to control the trade-off between privacy and model accuracy. These parameters determine the level of privacy protection for the data.
- **Select Differential Privacy Mechanisms**
  Choose appropriate privacy-preserving methods like the Laplace or Gaussian mechanism to add noise to data or model outputs. This ensures that individual data points remain protected.
- **Data Preprocessing**
  Anonymize and normalize the dataset to ensure that sensitive information is protected and the data is in a suitable form for applying differential privacy techniques.
- **Set Privacy Budget**
  Allocate the epsilon privacy budget to various queries or data operations. This helps control the amount of privacy loss allowed throughout the process.
- **Initial Testing**
  Apply differential privacy techniques to a sample dataset and evaluate their impact on data and model performance. This helps ensure that privacy is maintained without significantly compromising accuracy.
-

CONCLUSION

- In conclusion, Module 1 sets the foundation for implementing differential privacy by defining privacy requirements and selecting the appropriate privacy mechanisms. By preprocessing and anonymizing the data, the model is prepared to handle sensitive information securely. Setting the privacy budget ensures a balance between privacy and model accuracy, while initial testing helps evaluate the impact of privacy techniques on model performance. This module ensures that the data and model meet the necessary privacy standards before full-scale implementation.