Impact of Differential Privacy on Decision Tree Regression Performance

Prateek Majumder	Neha Roy Choudhury	Anshuman Jha	Divya kumar Sanghvi
Rahul Govind Kumar	Ayush Chakraborty	Piyush Sunil Borse	

Differential Privacy (DP) is a technique used to enhance data privacy by adding controlled noise to datasets, reducing the risk of individual data exposure. However, this comes at the potential cost of reduced data utility and model effectiveness. This report evaluates the impact of DP on Decision Tree Regression by comparing four different models trained on original and DP-processed datasets.

Methodology:

The analysis was conducted using a dataset containing advertising spending across TV, Radio, and Newspaper, with Sales as the target variable. The following steps were performed:

1. **Compute Basic Statistics**: Mean, standard deviation, and sum were calculated for the dataset before applying DP.
2. **Apply Differential Privacy**: Laplace noise was added to the independent variables (TV, Radio, and Newspaper) and the dependent variable (Sales).
3. **Train and Compare Four Models**:

   Model 1: Original Data Model – Trained on the original dataset without DP.
   Model 2: DP-Processed Data Model – Trained on the DP-processed dataset.
   Model 3: DP-Enhanced Training on Original Data – Trained on the original dataset with DP applied during training.
   Model 4: DP-Enhanced Training on DP Data – Trained on the DP-processed dataset with additional DP noise applied during training.

4. **Evaluate Model Performance**: Models were assessed using four key metrics:

   R^2 Score: Measures model accuracy (higher is better).
   MAE (Mean Absolute Error): Measures average absolute errors (lower is better).
   RMSE (Root Mean Squared Error): Penalizes large errors more than MAE (lower is better).
   MAPE (Mean Absolute Percentage Error): Measures relative prediction error as a percentage (lower is better).

Results:

📊 **Model Performance Comparison:**

Model	R^2 Score	MAE	RMSE	MAPE
Original Data Model	0.9311	0.9850	1.4748	8.89%
DP-Processed Data Model	0.8491	1.6360	2.1823	14.33%
DP-Enhanced Training on Original Data	0.9574	0.9025	1.1590	8.53%
DP-Enhanced Training on DP Data	0.8607	1.7080	2.0969	14.55%

Analysis & Insights:

A. Impact of Differential Privacy on Data Utility

1. The Original Data Model performed well with highest R^2 (0.9311) and lowest errors, showing that the unaltered dataset retains strong predictive power.
2. The DP-Processed Data Model showed significant accuracy loss (R^2 dropped to 0.8491, MAPE increased to 14.33%). This confirms that directly applying DP noise reduces data quality, impacting prediction accuracy.

B. Effectiveness of DP-Enhanced Training

1. DP-Enhanced Training on Original Data achieved the highest accuracy (R^2 = 0.9574) and the lowest error rates, outperforming the Original Data Model. This suggests that carefully applied DP during training can enhance model robustness without degrading accuracy.
2. The DP-Enhanced Training on DP Data model improved slightly over the DP-Processed Data Model (R^2 = 0.8607 vs. 0.8491) but still performed worse than models trained on unaltered data.

C. Worst-Performing Model: DP-Processed Data Model

1. Training directly on the DP-perturbed dataset led to the largest drop in performance, highlighting the negative impact of noise-induced distortions on model accuracy.

Key Takeaways:

1. Applying DP directly to data significantly reduces accuracy (R^2 drop from 0.9311 → 0.8491).
2. DP-Enhanced Training on Original Data improves performance over the standard model (R^2 0.9574 vs. 0.9311).
3. Applying DP to both data and training does not offer significant benefits and results in further accuracy loss.
4. For privacy-preserving ML, applying DP during training is better than perturbing the dataset.

Conclusion:

Differential Privacy offers a trade-off between data protection and model performance. While directly applying DP to the dataset results in a significant accuracy loss, DP-enhanced training on original data provides an effective way to preserve privacy while maintaining strong predictive performance.