AI Course Project

The goal of my project is to explore the application of local differential privacy in IoT systems with limited budgets. I implemented techniques such as local differential privacy using Laplacian Noise addition, FXP hardware Baseline, Thresholding, and Resampling as recommended in the research paper. My focus was on achieving a general implementation using the algorithms outlined in the paper.

Review

Integrating Resampling and Thresholding into Local Differential Privacy (DP) on Ultra-Low Power (ULP) hardware enhances privacy robustness. DP-Box, a specialized hardware solution, ensures effective data privacy and maintains high utility for sensor and IoT applications. It offers comprehensive support for aggregate statistics and machine learning tasks in privacy-sensitive environments.

Novelty

I have implemented Local Differential Privacy (LDP) using the Laplace noise mechanism on Fixed-point (FxP) hardware. Additionally, I integrated Thresholding, Resampling, and the DP-Box Algorithm as suggested in the research paper to ensure robust maintenance of local differential privacy.

Conclusion

DP-Box methods like resampling and thresholding exhibit impressive accuracy rates on large datasets like UJIIndoorLoc. Thresholding achieves a remarkable 99.32% accuracy, outperforming resampling slightly, which still achieves a high 99.12% accuracy. These results

underscore DP-Box's effectiveness in maintaining accuracy while ensuring privacy in extensive datasets through differential privacy techniques.

Dataset and Code References

[33] M. Lichman, “UCI Machine Learning Repository,” 2013.

[36] J. R. Quinlan, “Combining instance-based and model-based learning,” in Proceedings of the tenth international conference on machine learning, pp. 236–243, 1993.

[38] J. Torres-Sospedra, R. Montoliu, A. Mart´ınez-Uso, J. P. ´ Avariento, T. J. Arnau, M. Benedito-Bordonau, and J. Huerta, “UJIIndoorLoc: A new multi-building and multi-floor database for WLAN fingerprint-based indoor localization problems,” in Indoor Positioning and Indoor Navigation (IPIN), 2014 International Conference on, pp. 261–270, IEEE, 2014.