

A Unified View of Frequency Estimation and their Attacks on Local Differential Privacy



Al Mehdi Saadat Chowdhury, Dhaval Pankaj Tanna, Deepak Vellanki, Chirag Manjeshwar

School of Computing and Augmented Intelligence

Arizona State University

Outline

Introduction:

- Differential Privacy
- Local Differential Privacy
- Frequency Estimation and Pure LDP
- Attack Problem

Frequency Estimation Techniques:

- K Randomized Response (kRR)
- Optimized Unary Encoding (OUE)
- Optimized Local Hashing (OLH)

Attacks:

- Attack Types
- Attacking kRR
- Attacking OUE
- Attacking OLH

Defenses:

- ?
- ?
- ?

Evaluation:

- Comparison between Estimators
- Gain from Attacks
- Impacts of Parameters on Attacks

Conclusion

Introductory Concepts

Differential Privacy

Local Differential Privacy

Frequency Estimation Problem

Pure Local Differential Privacy

• A local mechanism is a function that takes a single record as input and returns a single record as output.

• A local mechanism is pure if it does not store any information about the data it has seen.

• A local mechanism is differentially private if it satisfies the differential privacy condition.

• A local mechanism is pure and differentially private if it satisfies the pure differential privacy condition.

• A local mechanism is pure and differentially private if it satisfies the pure differential privacy condition.

• A local mechanism is pure and differentially private if it satisfies the pure differential privacy condition.

• A local mechanism is pure and differentially private if it satisfies the pure differential privacy condition.

• A local mechanism is pure and differentially private if it satisfies the pure differential privacy condition.

• A local mechanism is pure and differentially private if it satisfies the pure differential privacy condition.

Attack – Problem Formulation

Frequency Estimation Techniques

K Randomized Response

Optimized Unary Encoding

Optimized Local Hashing

Efficiently handle large datasets with local hashing.

Local hashing reduces memory usage and speeds up search operations.

Learn how to implement and optimize local hashing in your applications.

Join us for this informative session!

Attacks on Frequency Estimators

Attack Types

Attacking kRR

Attacking OUE

Attacking OLH

Evaluation

Comparison between Estimators

Gain from Attacks

Impacts of Parameters on Attacks

Conclusion

Summary

Open Problems

Thank You