Isaias Rivera

CS 528 - Project Proposal

Local Differential Privacy and Federated Computations

The current dataset that I am planning on using is a collection of Fitbit device statistics. This dataset includes things such as calories burned, time sleeping, and time active. Given this dataset, I plan on simulating LDP for each user in the dataset, where a server can request values or computations to be run on any particular value. Each user would use an LDP method such as Generalized RR or a Basic RAPPOR. These responses could be compiled to generate an overall computation of a user database. An example of this would be to find the percentage of users who have less than a certain number of calories burned. Computations should disallow the ability to learn anything beyond the result of computations, meaning I will assume both parties are semi-honest. I can incorporate homomorphic encryption to prevent the user or server from knowing each other's inputs when performing computations. For each computation, I will discuss the differences between the true and generated values, including cases that use or don't use encryption.