Utilizing homomorphic encryption and acceleration framework on statistical machine learning methods for crash severity privacy

Team Member: Chinedu, Wei Chen

**Problem statement:**

Crash severity privacy is really common and hard to mitigate in every aspects releated to data. And security and privacy always the first consideration in machine interations.

**Goals/Objective:**

1. Comparison of the performance of each statistical machine leaning methods
2. Apply homomorphic encryption to improve data privacy and solve crash severity privacy.
3. Use TABLE Unified Template-based Framework to accelerate the execution of statistical machine learning methods

**Methods** we are going to utilize:

Acceleration method: TABLE Unified Template-based Framework.

Prediction method: Multinomial logit(MML), Near neignbor classification(NNC), Support vector machines (SVM), Random forests(RF)

Clustering method: K-means clustering (KC), Latent class clustering (LCC)

**Experiment plan**

we decide to make a survey of each of this statistical machine learning method, and try to find a better way to alleviate the affects from crash severity privacy problems. Homomorphic encryption and acceleration framework are two aspects we plan to explore and analyze