CS 6804: AI Technologies for Cybersecurity Defenses

Project Title: **Learning through joint datasets using differential privacy to each dataset separately**

Student: Tanmoy Sarkar Pias

1. What are you trying to do?

Let's say, ten different hospitals have their own dataset of their cancer patient. Each hospital can use their own dataset to build a machine learning model as the dataset is secured within that particular hospital. But a more robust machine learning model could be built by aggregating all the datasets from those ten hospitals but the patients' sensitive information have to be shared with other medicals. So, to solve this problem, I am trying to create a privacy-preserving machine learning model that is trained on all of the datasets where differential privacy is applied on each dataset separately before the aggregate training process.

2. How is it done today, and what are the limits of current practice?

Currently, this is done by using a third party that aggregates all the data for training machine learning model.
The limitation of this system is that the third party should be trustworthy as it has the medical records from all the hospitals.

3. What is new in your approach?

I will use differential privacy on each dataset then aggregate all the datasets for training with a global ML model. So that, perturbed noise is less than local differential privacy where individual information is perturbed.

4. What's your evaluation plan (when applicable)?

I will compare model accuracy using the stated approach with the traditional approach where local differential privacy is used. Intuitively, the proposed approach should work better as less noise is added to anonymize the data.