1. **Federated Machine Learning in Intelligent Transportation System.**

In the past few years, we can see the rapid growth in the autonomous vehicle system. The growth of ML and DL have powered up the automation of these vehicles. ML and DL are widely used for Destination prediction, Traffic flow prediction, Traffic Signal Control. The traditional ML and DL techniques require the aggregation of data from these vehicles to perform these applications. This data ranges from GPS data to wireless sensor data. These data are very sensitive in nature and when exposed to the hackers may be disastrous. In this project, we will be working on Federated Machine Learning techniques to perform these applications without compromising the users data.

2. **Adversarial Deep learning in Intelligent Transportation System.**

We can see various applications of DL in the Intelligent Transportation system which are described above. Fully automated vehicles are highly powered up by Deep learning algorithms. One example is detecting the use of computer vision in automated driving. However, when we bring a small perturbation in the dataset, DL algorithms suffer from high false positive rates. The perturbations are very much possible if the dataset which powers up these autonomous vehicles are coming from a decentralized environment. In this research project we explore many possible perturbation techniques in DL and build algorithms to defend it.