Abstract for ML project

Our team:

Gautam Arora – 20BAI1053
Narayan Subramanian – 20BAI1207
Sarvesh Chandak – 20BAI1221

Topic - Heart disease prediction

Cardiovascular diseases (CVDs) are a group of disorders involving the heart and blood vessels. They are the number one cause of death globally, taking an estimated of 17.9 million lives each year, which accounts for 31% of all deaths worldwide. Among these, 38% people were under the age of 70 years. Stroke, heart failure, arrhythmia and myocardial infarction are some of the most common cardiovascular diseases with high mortality rates around the world.

Early detection of heart diseases is critical in the treatment and management of cardiovascular diseases, wherein machine learning can be a powerful tool in detecting a potential heart disease diagnosis. But they are not detected in the early stages due to the impractical costs of the tests available. Thus, a fast, real-time and reliable system that predicts the chances of a patient having heart disease in an optimized manner is required.

Along with this, we will try to build up a robust model which will defend against adversarial efforts. At present, there are very small percentage of current AI research which goes towards defending AI systems against adversarial efforts. Some systems already used in production could be vulnerable to attack. Machine learning algorithms are developed to assume that the environment is benign, but they fail when even a small adversary can modify their inputs. This is where adversarial machines come in handy. Adversarial machine learning is a branch of machine learning that studies a set of assaults aimed at degrading the performance of classifiers on certain tasks. Adversarial machine learning ensures the machine leaning model’s resilience.