Privacy Enhancing Technologies
Project Report

Group Members:
Muhammad Hassan Rashid (7001957)
Kinaan Aamir Khan (7011611)
Noor ul Ain (7015655)

Model Inversion:

The target model accuracy of model inversion was 95%.

The attack model performance is given below.

Since the dataset was very small the result is not upto the mark.

Membership Inference

We report this performance on the dataset of the target model.
The attack model performance is 85.61%.