Biography
Nirvan Tyagi is pursuing his PhD in Computer Science at Cornell University under Prof. Tom Ristenpart working in the Security & Privacy group located in the NYC Tech campus. His research interests lie broadly in building and reasoning formally about secure, privacy-preserving systems with past work in anonymous communication, secure cloud storage, and machine learning privacy. As a DLI fellow, Nirvan aims to investigate forms of training data leakage in machine learning algorithms.

Abstract
In this talk, Nirvan will give a broad survey of some of the security and privacy concerns with use of machine learning that make up the focus of recent research in the area. Topics covered include “fooling” machine learning models, “stealing” machine learning models, and understanding what information is “leaked” by machine learning models about the (potentially sensitive) data they are trained on.