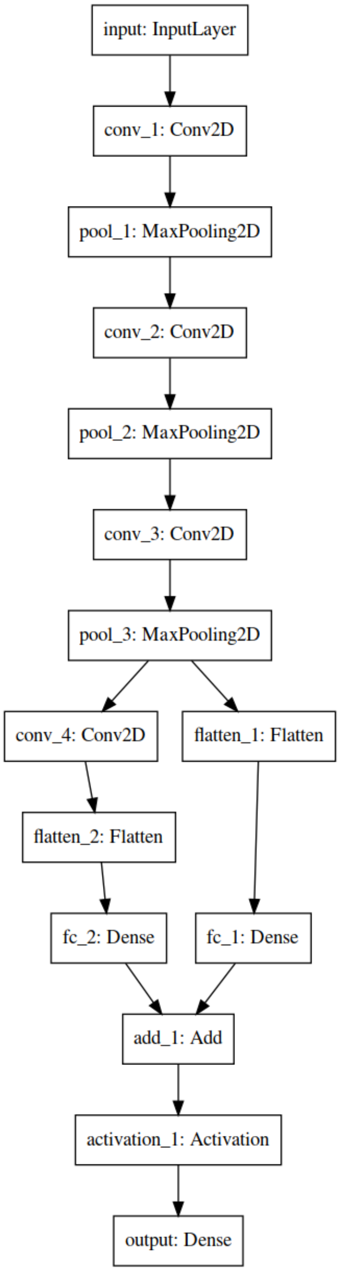
Lab 2 : ECE-GY 9163 Machine Learning for Cybersecurity
Submitted by: Ali Quidwai (maq4265)

GitHub Link: https://github.com/Ali-Maq/Lab_02_CSML

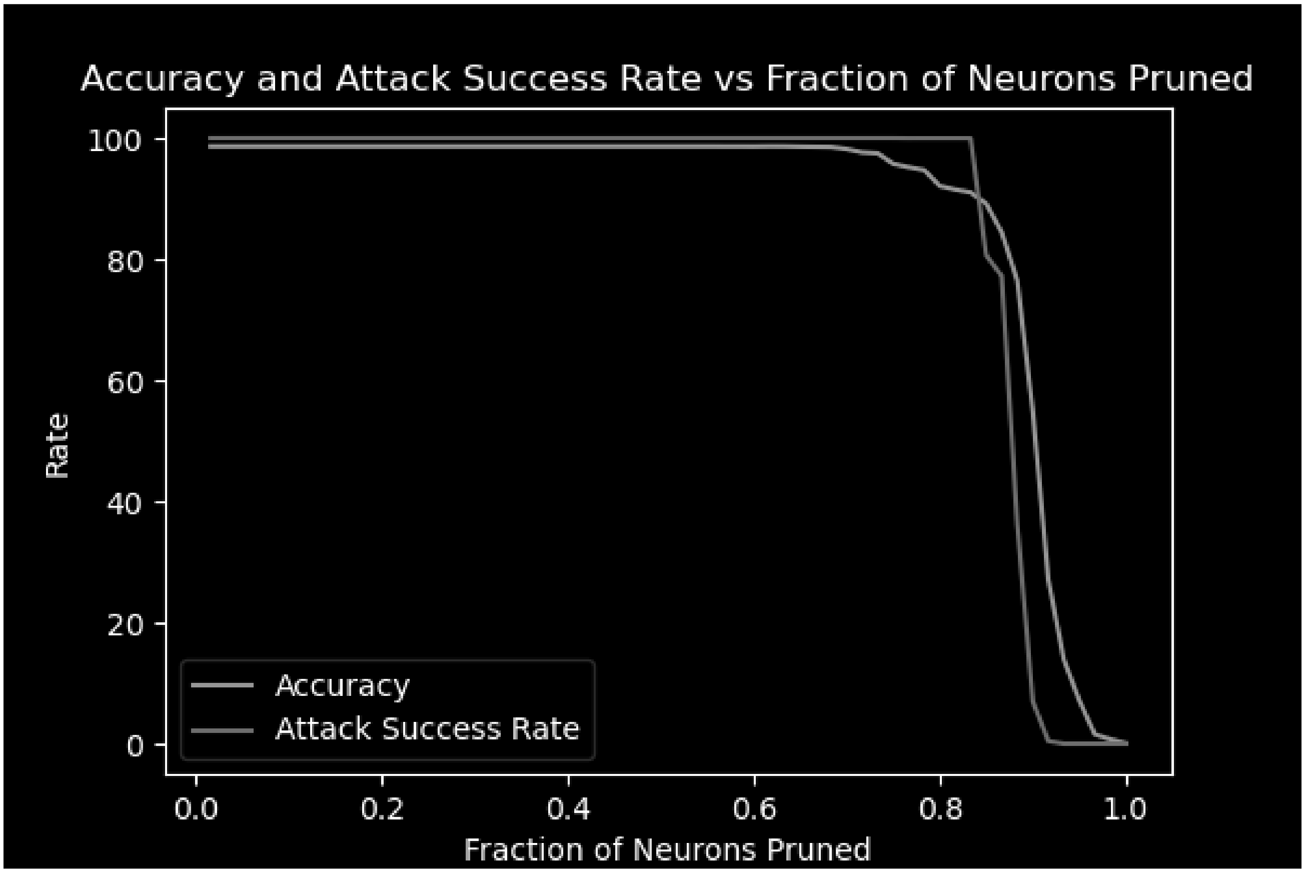
The model architecture (B) is shown below:



The table below shows the accuracy on clean test data and the attack success rate (on backdoored test data) as a function of the fraction of channels pruned (X):

	B Prime Model			Retrained Net			B model
X	2%	4%	10%	2%	4%	10%	
Clean Accuracy	95.90	92.29	84.54	95.74	92.12	84.33	98.62
Attack Success rate	100.0	99.98	77.20	100.0	99.98	77.20	100.0

The graph for the above table is as follows:


Accuracy and Attack Success Rate vs Fraction of Neurons Pruned
Rate
Fraction of Neurons Pruned
Accuracy
Attack Success Rate