Assignment 1: Model building

Innopolis University

The security and interpretability of machine learning 2021 - Bachelors

20 points

1 General Instructions

In this assignment, you are going to build the model that you will be using during this course for the upcoming homeworks ans final project. You are required to submit your solutions via Moodle as a single ipynb file. Do not forget to include your name in the submitted document.

The source code should contain adequate internal documentation in the form of comments. Internal documentation should explain why and how you apply the instructions.

Plagiarism will not be tolerated, and a plagiarised solution will be heavilypenalized for all parties involved. Remember that you learn nothing when you copy someone else's work, which defeats the exercise's purpose! You are allowed to collaborate on general ideas with other students as well as consult books and Internet resources. However, be sure to credit all the sources you use to make it clear what part of your solution comes from elsewhere.

1.1 Model Creation (20 points)

First, you are encouraged to choose building a model for a task that you find interesting.

For those who did not choose a task, you are asked to build, train, and evaluate one of these models

1. A CIFAR-10 classifier.
2. A malware detection system

If you choose the malware detection systems, you can look at " https://github.com/elastic/ember " as a starting point.