Security of Big Data Analytics

Laboratory 06: Analysis of data sets using artificial intelligence mechanisms

First name: Mateusz Last name: Wisniewski

Index number: 148327 Exercise date: 20.11.2024

Used Lab equipment:

Group members:

Report submission

The document containing the exercise instructions includes active text fields where answers to the provided questions must be entered. As a result, once all answers are filled in (along with personal information of the individual completing the exercise), the document transforms into a report. It's recommended to open the file using Adobe Acrobat, or browsers such as Firefox or Chrome.

If you wish to maintain the functionality of the text fields after saving the file (allowing for future changes), avoid selecting the 'print to PDF' option when saving the file to your disk. For added safety against potential loss of entered data due to system crashes, save the file periodically.

Final report should be composed of the following files:

000000_SBDA_06_01.pdf (student ID: 000000, Lab number 06, file number 01) - main raport file (this file)

000000_SBDA_06_02.ipynb (student ID: 000000, Lab number 06, file number 02) - Jupyter Notebook file with all results (code, comments, answers)

000000_SBDA_06_03.html (student ID: 000000, Lab number 06, file number 03) - Jupyter Notebook file downloaded as HTML

All files should be added to the 7zip archive (final archive, ready to upload to Moodle system):
000000_SBDA_06.7z (student ID: 000000, Lab number 05, 7zip archive)

Prepare environment

Before starting a series of laboratory exercises on the security of Big Data analysis, the required environment must be prepared. The exercises will be implemented in Python language. Therefore, check if the Anaconda environment is installed on your computer along with the Jupyter Notebook editor.

If Anaconda is installed - check for available updates and update the environment. If the Anaconda environment is not available - install it.

To complete this and the next exercise, you must install the Secml library (secml: A Python Library for Secure and Explainable Machine Learning, Melis et al., arXiv preprint arXiv:1912.10013 (2019).).

To install the library, follow the description presented on the page:
https://secml.readthedocs.io/en/v0.15/

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

If you cannot install the secml library, ask your teacher to provide you with a virtual machine with a ready-made environment.

Lab scenario

Download file SBDA_06.ipynb from Moodle system and open it in Jupyter Notebook. If you wast to see content of SBDA_06.ipynb without opening it in Jupyter Notebook, please see file SBDA_06.pdf, Perform the exercises according to the instructions contained in it.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

Additional notes

If provided space for an answer is insufficient, use this additional space.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.

The project "Cyber Security for the European University EUNICE", implemented under the National Academic Exchange Agency's Strategic Partnerships Programme. Implemented in cooperation between the Poznan University of Technology and the University of Catania, University of Mons, and Brandenburg University of Technology.