Spring 2023 CIS 735 Machine Learning for Security
Project 2
Syracuse University

Due date and time: The deadline to submit the final project report is by Wednesday, April 19, 2023; 11:59 pm.

This assignment addresses an important aspect of graduate education in general and this 700 level course in particular to develop the ability to define research and technical problems (projects) and develop solutions to these problems.

Background Information

The file "data Description" gives the details of data collected from 17 individuals. The data has accelerometer and gyroscope readings from Google Glass and two mobile phones- one in the front pocket and one in the back pocket.

What do you have to do?

Define a project that can use the data given in the **Background Information** and execute the project. Note that you must define your own problem. For example, you could choose to separate the head and torso movement data from Google Glass or you could predict phone data from Google Glass data or vice versa or you could use deep learning methods to generate additional samples from one modality or another modality. Or you could use Explainable AI for deep learning models to explain which features affect authentication in [1]. The preceding examples are just some samples of problems. I encourage you to define your own problem.

What should be included in the report?

(200 words) Define the problem.

(200 words) Describe the solution.

(1000 words) Carry out your solution and substantiate. Explain the results, for example give tables and graphs in support of your results.

You may format your report on the lines of the paper [1] related to this work. *A report more than six pages (does not include references) will result in penalty in grades.*

If I notice any "copy and paste" in the report from external sources, the penalty is zero for the assignment.

Include a cover page containing the title of the project or paper and a list of the team members in the group. List the contributions of each group member.

Submit only one file (project report) per group.

What should you submit?

Your submission should include:

(1) A report as above.

(2) An executable including any dependencies in a format that I or the TA can run the code all files necessary to run the code) and a brief project report. A small Readme file (or a user manual) that tells me how to execute the code. What is the input and what type of output I can expect.

Submission Details

You are allowed to work in groups of not more than three students.

Name the report file as: Last name-final report. If there is more than one person in the group then use both names in the last name part of the report name. For example, if two students with last names, Smith and Adler are submitting the report than the file name should be *Adler-Smith- MLSecurity-final.pdf*. If three students are submitting the project report then add the third last name also.

In a zip file, upload any supporting material, for example simulation code or a .exe file.

References

[1] Parimi, Gayathri Manogna, Partha Pratim Kundu, and Vir V. Phoha. "Analysis of head and torso movements for authentication." *2018 IEEE 4th International Conference on Identity, Security, and Behavior Analysis (ISBA)*. IEEE, 2018.

Also read the paper given through the following link.

https://www.sigplan.org/Resources/Advice/Pugh/