EnnCore Kick-off meeting

Date: 12/02/2021

Participants:

Andre Freiras (UoM)

Xiaowei Huang (UoL)

Mustafa Mustafa (UoM)

Mikel Lujan (UoM)

Gavin Brown (UoM)

Edoardo Manino (UoM)

Somayeh (Urbainchain)

Notes:

1. Lucas suggested saving the slides of our kick-off meeting at <https://livemanchesterac-my.sharepoint.com/personal/lucas_cordeiro_manchester_ac_uk/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Flucas%5Fcordeiro%5Fmanchester%5Fac%5Fuk%2FDocuments%2Fkick%2Doff%2Dmeeting>
2. Every participant agreed to meet once a month to discuss our progress over the project’s milestones and stimulate interactions among the separate work packages. Andre pointed that the communication should be more intensive among the work packages, i.e., we don’t need to wait for the monthly meeting to interact with other work packages.
3. Mikel also suggested having a reading group about the EnnCore project once a month. In this reading group, we should indicate the key papers related to the EnnCore project.
4. We will consider Edoardo in the WP1 to support Mustafa in writing the use cases. Our partners should provide a short description of the use cases, which should answer the following questions: Which kind of data? Which type of features? What do they want to achieve?
5. Mustafa suggested developing a threat modeling using data from diagrams from these use cases. Mustafa is very familiar with the use cases from Urbanchain.
6. Andre suggested scheduling some meetings to discuss the use cases. Andre suggested having a first version of the use case description soon.
7. Xiaowei is primarily working on verifying AI models, particularly for image data/classification. Xiaowei mentioned that extending from image data to general data might take some considerable effort. For example, for the Urbainchain case, we’ll have to update the system when the new data is coming, which involves low-dimensional data.
8. We should investigate the link between Explainable AI and formal verification. How can XAI be used? How could formal verification help in XAI?
9. Mustafa mentioned there would be different levels of explainability. One group of explainability could provide enough information for one particular user, but not for other users.
10. Andre mentioned that we need to define explainable AI formally.
11. We discuss working on three primary papers for the first year of the project: (1) the world of XAI and formal verification (natural language processing). (2) Consider use cases or standard benchmarks and evaluate the available tools to verify those use cases and benchmarks. We should identify the existing gaps from the current literature. (3) Formal verification + abstract interpretation for recurrent neural networks.
12. Our next meeting will take place on March 19th, Friday at 4 pm. One hour for the reading group and one hour for the project follow-up.

Links provided

Standard ML benchmark for training and testing

(old website <https://mlperf.org/>) <https://mlcommons.org/en/> with training at

<https://mlcommons.org/en/news/mlperf-training-v07/> and inference at <https://mlcommons.org/en/news/mlperf-inference-v07/>

<https://github.com/TrustAI/DeepConcolic>