PhD Call

Title: PhD positions on robustness and security testing of AI based systems

Deadline: September 30th, 2023

Abstract:
The TAU (Testing Automated) research group at the Software Institute of Università della Svizzera italiana (USI) investigates novel testing techniques to improve the robustness and security of systems based on deep learning. We offer two PhD positions in the following topics: (1) search-based test case generation for vulnerability exposure in deep learning based systems and creation of a robustness assessment benchmark; (2) automated partition of a complex input space into a topographical map consisting of regions that maximise the likelihood of fault exposure when test cases are sampled from unexplored or boundary map regions. Correspondingly, the first PhD position is funded by the Horizon European project Sec4AI4Sec which aims to support security testing of AI-based systems; the second is funded by the SNSF project Toposcope, aiming at redefining the testing activities as the exploration of a topographical map of the input space.

We are scouting excellent applicants for these two PhD positions. Successful candidates will work at Università della Svizzera italiana (USI) in Lugano, Switzerland, under the supervision of prof. Paolo Tonella and the co-supervision of Dr. Nargiz Humbatova and Dr. Jinhan Kim. At USI, PhD salaries are highly competitive (around 50 kCHF), in accordance with the Swiss standards. Ideally, the selected candidates are expected to start on October 1st, 2023, but later starts can also be considered. The duration of the PhD contract will be 4 years.

Applications for PhD positions should include a curriculum vitae and the exam transcripts. PhD candidates should hold an MSc degree in Computer Science by Fall 2023. Applications can be sent to paolo.tonella@usi.ch. The call will remain open until all positions are filled, but priority will be given to earlier applications.