Introduction to the Artificial Intelligence Security: Ensuring Safety, Trustworthiness, and Responsibility in AI Systems Minitrack

Tyson Brooks
Department of Defense and
Syracuse University
ttbrooks@syr.edu

Shiu-Kai Chin
Syracuse University
skchin@syr.edu

William Young
Syracuse University
weyoung@syr.edu

Erich Devendorf
Air Force Research Laboratory
erich.devendorf.1@us.af.mil

The Artifical Intelligence Security: Ensuring Safety, Trustworthiness, and Responsibility in AI Systems minitrack serves as a platform for presenting innovative research, discussing emerging trends, and setting the agenda for future exploration in the field of AI security. It will address the intersection of technology, safety, trustworthiness, responsibility, and policy, ensuring a comprehensive approach to AI security. As networks and devices will rely heavily on AI machine and deep learning algorithms, these networks and devices should be able to resist the various AI cyber-attacks such as hacking of networks, devices, theft of information, disruption, etc. and be able to continue performing under severe environmental conditions. Through machine learning algorithms over the transmitted information, the miscoding and leaking of information during transmission channels must monitor any loss, miscoding and leaking of data. Timely adjustments of information with falling quality and automatic switching to the best routing IoT systems by making uses of multi-directional routing is also warranted. AI security will need to provide the principles and technologies to unify these systems to deliver the end-state goal of secure systems for greatly enhanced interoperability, scalability, performance, and agility.

URI: https://hdl.handle.net/10125/109688
978-0-9981331-8-8