conferenceseries.com

11th Global Summit on Artificial Intelligence and Neural Networks

August 31, 2023 | Webinar

Security of AI play a key role to show it a Majesty or a Monster power - Data poisoning and Adversarial Machine learning.

Mohammadsadegh Vahidi Farashah

Cyber Security | Project Manager | AI/ ML Researcher | Clinical Informatics, Canada

Nowadays AI play a key role in our life and show that can manage all of the things in the future. Human communication interaction (HCI), face and speech recognition guidance, self-driving cars and healthcare systems as well as a lot of amazing topics in using AI show the significant power of AI in the future of our lives. We can use AI for cyber security to detect different attacks such as spam detection and behavior analysis to detect anomalies in networks and users activities as well. The big question is who can ensure the security of AI itself?, and what will happen if the AI algorithms and detections tampered with wrong data and give the wrong command to connected devices, cars and models poisoned? Data poisoning and adversarial machine learning is an example of that we want to discuss more about them. Adversarial examples are specialized inputs created with the purpose of confusing a neural network, resulting in the misclassification of a given input. These notorious inputs are indistinguishable to the human eye, but cause the network to fail to identify the contents of the image. Data poisoning means attackers tamper with the training data used to create deep-learning models. This action means it is possible to affect the decisions that the AI makes in a way that is hard to track. In addition, these experts are racing to protect AI from hackers. It is an adversarial attack that tries to manipulate the training dataset and data masquerading in order to control the prediction behavior of a trained model such that the model will label malicious examples into a desired class.

Biography

Mohammadsadegh Vahidi Farashah is a Senior Cyber Security Project Manager at MCI and an AI/ML consultant member of Endocrinology and Metabolism Research Center at Hormozgan University of Medical Sciences. With over 10 years of experience working at MCI and 4 years of experience in AI/ML, Mohammadsadegh is a seasoned professional with a deep understanding of the cyber security and the potential of AI/ML to drive innovation and growth.

sadegh.vahidi@gmail.com