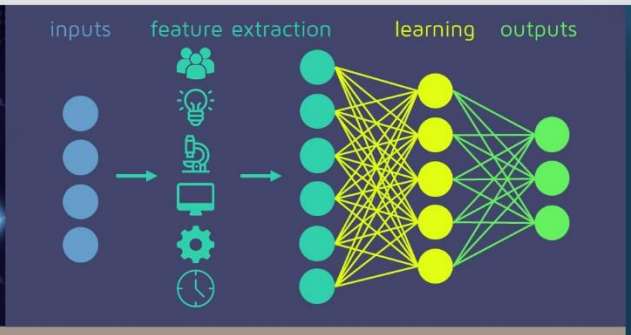
ICAC

SLIIT

Workshop on

ML4Sec: Workshop on Using Machine Learning for Cybersecurity



The use of machine learning in cybersecurity is a fast-growing trend. With the recent advances in machine (and deep) learning technologies, many security practitioners began to believe that these technologies can solve all of our cybersecurity problems. Enterprise security vendors started to integrate these technologies into their security solutions. Despite extensive academic research, however, they are not yet widely used in our production environments. This is due to several key challenges, such as zero-days, concept drift, and noisy features that hamper the success of these technologies in security problems. Most of these security inventions do not learn in the customer environment, but train on multiple data samples in a vendor's cloud and download to client companies following a very similar approach to traditional antivirus solutions. Therefore, they are not fundamentally different from signature-driven methods. ML4Sec offers a dedicated forum to discuss these open issues, challenges and innovative approaches. The main aim of this workshop is to promote this research area with some hands-on experience for the delegates. Participants will have the opportunity to work on a security analytic problem, in both defensive and offensive perspective, while highlighting the latest trends in the field. As a result, we expect attendees to better understand a wide variety of machine learning methods and tools available for cybersecurity problems and appreciate the exciting new use cases and challenges in this research area.

Speakers:

Mr. Chamath Palihawadana is a research assistant in the School of Computing at Robert Gordon University (RGU) with a focus on providing AI as a service on web platforms.

Dr. Omar Alkadri is a Lecturer in Cyber Security in the School of Computing at RGU. He has extensive research experience in cyber security and wireless communications and published in numerous international conferences and journals.

Dr. Harsha Kalutarage is a Lecturer in Cyber Security in the School of Computing at RGU. He has 10+ years of research experience in cyber security threat intelligence using machine (and deep) learning technologies, has produced 40+ publications and a patent, and has delivered several research projects in this area to industrial partners.

WORKSHOP

The International Conference on Advancements in Computing 2020

10th Dec. 2020

zoom

3.45 pm to 4.45 pm