Workshop Title:

The 4th Workshop on Machine Learning for Web Services Security

Abstract:

Cyber security domain is pivotal for the world today due to its significance for the computer centric social and business world. The domain poses numerous challenges, such as threat detection, privacy presentation, intrusion detection, etc. With the rapid growth of cyber world and the subsequent development of adversarial techniques, current cyber-threats are becoming more and more complicated and complex. For instance, for web services available over the internet via the World Wide Web and through other internet-based systems and protocols. For the improved and efficient usage of the cyber technologies, Web Services Security (WSS) is an important area for the cyber-security researchers in order to define security measures that prevent them from cyberattacks. However, it is challenging to achieve in the spectrum of paradigms in technologies providing us services through complex systems. Therefore, the explosion of web-based services has created unprecedented opportunities and thus essential security challenges. The aim of this workshop is to provide a premier international platform for the wide range of experts including practitioner and academicians an essential linkage to web services, services science, and service orientation in most current IT-driven collaborations. This workshop will focus on overfitting issues, such as architecture cost, design, algorithms and methodologies to solicit original research work with a particular emphasis on the challenges and future trends in cyber security, particularly for web-based services security, using machine learning applications. Machine learning approach has proven to be suitable for the WSS because it can help learn information and behaviour from the online and offline data sources in an automatic routine and reduce the workload of security threat analysis through human experts. In connection to this, emerging approaches, such as

reinforcement learning, adaptive learning, deep learning, etc can be used for efficiently detecting any type of cyberthreat to WSS.

We invite researchers to contribute original research papers and review articles that will seek high-quality contributions regarding the recent advances in applying machine learning for solving cyberthreat for WSS challenges. Topics of interest include, but are not limited to ones listed below.

- Deep learning techniques in security and privacy.
- Reinforcement learning in security and privacy
- WSS threat and attack model generation based on machine learning
- Adversarial machine learning in WSS
- Insider threats and countermeasures
- Web semantics security
- Web services-based Biometrics security
- Personal data protection over WSS
- Ethical and legal implications of security and privacy in web services
- Critical infrastructure protection in WSS
- Security and privacy prevention in web services
- WSS privacy policies
- Secure web services development methodologies and modelling
- WSS challenges and future trends

Workshop Chairs:

Asad Masood Khattak, Zayed University, UAE

Sajid Anwer, Institute of Management Sciences, Pakistan

Zeeshan Pervez, University of the West of Scotland, UK