Call for Papers

IEEE Workshop on Data Science for Cyber Security (DS4CS)

Important dates

Workshop papers' deadline:
March 15, 2023 AoE
Workshop authors' notification:
April 1, 2023 AoE
Camera-ready submission:
April 15, 2023 AoE
Early registration deadline:
May 5, 2023 AoE
Workshop dates:
July 31 - August 2, 2023

Workshop chairs

Anish Jindal, UK
Spiros Skiadopoulos, GR
Christos Tryfonopoulos, GR

Publicity chair

Paraskevi Raftopoulou, GR

Contact us

anish.jindal@durham.ac.uk
spiros@uop.gr
trifon@uop.gr
praftop@uop.gr

Program committee

Christos Anagnostopoulos, UK
Gagangeet Singh Aujla, UK
Denilson Barbosa, CA
Srikanta Bedathur, IN
Giampaolo Bovenzi, IT
Theodore Dalamagas, GR
Christos Dimitrakakis, NO
Gabriel Ghinita, US
Aris Gkoulalas-Divanis, US
Antonios Gouglidis, UK
Mouna Kacimi, IT
Panos Kalnis, SA
Gjergji Kasneci, DE
George Kollios, US
George Lepouras, GR
Dongzhu Liu, UK
Ida Mele, IT

Over the years cyber-threats have increased in numbers and sophistication; adversaries now use a vast set of tools and tactics to attack their victims with their motivations ranging from intelligence collection to destruction or financial gain. Lately, the introduction of IoT devices on a number of domains, ranging from smart applications (e.g., smart cities/grids/agriculture) to goods and infrastructure monitoring (e.g., transportation/logistics/power monitoring), has created an even more complicated cyber-defense landscape. The sheer number of IoT devices deployed globally, most of which are readily accessible and easily hacked, allows threat actors to use them as the cyber-weapon delivery system of choice in many today's cyber-attacks, ranging from botnet-building for DDoS attacks, to malware spreading and spamming.

Staying on top of these evolving cyber-threats and protecting the underlying equipment have become increasingly difficult tasks that nowadays entail the collection, analysis, and leveraging of huge volumes of data and require methodologies and techniques located at the intersection of statistics, data mining, machine learning, visualization and big data. Although the application of Data Science methodology to the Cyber Security domain is a relative new topic, it steadily gathers the interest of the research community as showcased by the utilization of data science techniques in a variety of cyber-defense facets that include proactive technologies (e.g., cyber-threat intelligence gathering and sharing), platform profiling (e.g., trust calculation and blacklisting), attack detection/mitigation (e.g., active network monitoring, situational awareness, and adaptable mitigation strategies), and others. This workshop aims to spotlight cutting-edge research in data science driven cyber-security and this year it emphasizes on the usage of such techniques on important applications such as drone/fleet/vehicle management, transportation/logistics/ supply chain monitoring, and smart cities/agriculture/mobility.

Prospective authors are encouraged to submit previously unpublished contributions from a broad range of topics, which include, but are not limited to, the following:

- Big data-driven cyber-security (incl. analytics and management)
- Machine and deep learning methods for cyber-security (incl. malware/phishing/botnet/ spam/intrusion/anomaly detection)
- Visualization methods (incl. visual situation awareness, VR & AR visualization, real-time visualization)
- AI-driven cybersecurity
- Private/sensitive information operations (inlc. retrieval, protection, extraction)
- Cyber-threat intelligence collection, identification and sharing at scale
- Machine-learning powered security (incl. traffic analysis, attack modelling, platform profiling and trust management)
- Advanced attack detection and mitigation
- Data science driven cyber-security for smart applications (incl. mobility/agriculture/ cities)
- Data science driven cyber-security for monitoring and management (incl. fleet/drone/ vehicle/transportation/logistics/ supply chain)

IEEE
IEEE SMC Systems, Man, and Cybernetics Society
IEEE SMC Technical Committee on Homeland Security
LOGOS RI RESEARCH&INNOVATION

Dimitris Michail, GR
Antonio Montinieri, IT
Luis Munoz-Gonzalez, UK
Kim Pecina, DE
Nikos Platis, GR
Panagiotis Rizomiliotis, GR
Nguyen Truong, UK
Theodora Tsikrika, GR
Sandeep Shukla, IN
Giannis Tsimperidis, GR
Thanasis Vergoulis, GR

Submitted manuscripts should not exceed 6 pages (plus 2 extra pages, being subject to overlength page charges) and should be of sufficient detail to be evaluated by expert reviewers in the field. The workshop's proceedings will be published by IEEE and will be included in IEEE Xplore. Detailed information about the paper submission and guidelines to authors can be found at the workshop's website https://www.ieee-csr.org/DS4CS.