The 21st IEEE International Conference on Machine Learning and Applications (IEEE ICMLA 2022)

Special Session on: **Cyber Security and Big Data**

December 12-15, 2022, The Bahamas, Caribbean

https://www.icmla-conference.org/icmla22/

Background and Aims

Big data represent a new challenge to cyber security. For instance, self-driving cars are predicted to produce 4000 GB of data per hour of driving. Furthermore, the Internet of Things is expected to generate 400 zettabytes (ZB) of data a year. In this emerging context, big data analytics represent a emerging analytical technology with the potential to offer the capability to collect, store, process, and visualize these vast amounts of data.

Big Data Analytics in cyber security examines security challenges surrounding big data and provides actionable insights that can be considered in order to improve the current practices related to the plethora of aspect cyber security related, for instance from the network operators, administrators and end users point of view.

The application of big data analytics in cyber security is critical. By exploiting data from infrastructure, computers, cyber physical systems, big data analysts are able to discover useful information from data in order to securize system also from both administrators and end users. Decision makers can make more informative and conscious decisions through this kind of emerging analysis, including what actions need to be performed, and improvement recommendations to policies, guidelines, procedures, tools, and other aspects of the security processes.

Scope/Topics

Submissions are expected from, but not limited to the following topics:

- Analysis, Design and Assessment of secure systems
- Security and privacy in Internet of Things (IoT)
- Securing private data on mobile devices
- Security in Cyber Physical Systems
- Security in Smart Grid
- Security in Cloud Computing environments
- Security in Social Networks
- Intrusion Detection
- Cyber Insurance

- Malware analysis
- Forensics
- Network security and Verification and Validation of Critical Infrastructures
- Design and validation of malware detection approaches and systems
- Security issues in Complex System and Environment
- Methodologies to the development and the analysis of secure systems

Submission Guidelines and Instructions

Papers submitted for review should conform to IEEE specifications. Manuscript templates can be downloaded from IEEE website[1]. The maximum length of papers is 8 pages. All the papers will go through the double-blind peer-review process. Authors' names and affiliations should not appear in the submitted paper. The authors' prior work should be cited in the third person. Authors should also avoid revealing their identities and/or institutions in the text, figures, links, etc.

Paper Publication

Accepted papers will be published in the IEEE ICMLA 2022 conference proceedings (published by IEEE). A selected number of accepted papers will be invited for possible inclusion, in an expanded and revised form, in some journal special issues.

Important Dates:

- Submission Deadline: September 9, 2022
- Notification of Acceptance: October 7, 2022
- Camera-ready papers & Pre-Registration: October 14, 2022

Special Session Organizers/Chairs:

Francesco Mercaldo, University of Molise, Campobasso, Italy and IIT-CNR, Pisa, Italy
Email: francesco.mercaldo@unimol.it
Special Session contact e-mail: francesco.mercaldo@unimol.it

Programme Committee

Fabio Di Troia, San Jose State University, United States

Alberto Ferrante, Università della Svizzera Italiana, Switzerland

Vincenzo Gulisano, Chalmers University of Technology, Sweden

Giacomo Iadarola, IIT-CNR, Italy

[1] www.ieee.org/conferences_events/conferences/publishing/templates.html

Longquan Jiang, Macrowing, China

Andrea De Lorenzo, University of Trieste, Italy

Ilaria Matteucci, Istituto di Informatica e Telematica, CNR, Italy

Eric Medvet, University of Trieste, Italy

Xuan Sun, Sanda University, Shanghai, China

P. Vinod, Cochin university of science and technology, India