Special Session on
Enterprise AI/ML for Zero-Trust or Zero-Leakage Cybersecurity Analysis
at
16th International Conference on Information Assurance and Security (IAS)
on
World Wide Web
December 14-16, 2021

http://www.mirlabs.org/ias21/

Objectives and Scope

Zero-Trust and Zero-Leakage security are latest cybersecurity buzzwords serve as a stimulus for new cybersecurity strategies in the age of enterprise cloud computing. Many of the security vulnerabilities can be addressed by implementing Zero-Trust and Zero-Leakage techniques. Zero-Trust security strategy demands that nothing within an enterprise's cloud or in a data center is accessible unless explicit authentication and authorization is granted. In Zero-Trust, a unique protect surface is made up with the organization's most vital and valuable data, assets, applications, and services (DAAS). The Zero-Leakage security policy prohibits data from being transmitted outside of the enterprise's cloud in any illegal manner, whether mistakenly or intentionally. Zero leakage security prevents unauthorized hackers from gaining access to sensitive data and prevents employees with access to sensitive data from unintentionally or maliciously allowing it to be accessed. Enterprise AI/ML appears to be less trustworthy due to security concerns in the cloud which needs more scalable, on-demand, and cost-effective option. The objective of this special session is to bring together researchers and practitioners interested in the development of intelligent cybersecurity frameworks, specifically the Zero-Trust, Zero-Leakage, and protect surface.

Subtopics

The proposed session welcomes research in the following areas.

- Artificial intelligence/machine learning-based cyber threat analysis
- Machine learning applications to Zero-trust or Zero-Leakage security and data-driven security
- Zero trust and/or zero leakage security architecture or models for forecasting lateral cyber-threat movement within a network
- Intelligent information assurance, verification, and validation in cloud security
- Semantic modeling, data representation and fusion for CTI Models that take into consideration

- Detection or mitigation of deception and uncertainty in cyber-attack vector or protect surface
- Visualization techniques for Zero-Trust or Zero-Leakage security intelligence analysis
- Ethical factors in intelligence cybersecurity analytics
- Other data analytics or algorithms for Zero-Trust or Zero-Leakage security (e.g. intelligent protect surface detection)
- Probabilistic models for Zero-Trust or Zero-Leakage intrusion and anomaly detection and prevention
- Zero-Trust or Zero-Leakage security architectures and adaptation with intelligent system

Paper Publications

- Proceedings will be published in Lecture Notes in Networks and Systems, Springer (Indexed in SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago)
  https://www.springer.com/series/15179
- Papers maximum length is 10 pages
- Papers must be formatted according to Springer format (Latex/word) available at: https://www.springer.com/de/authors-editors/book-authors-editors/manuscript-preparation/5636#c3324

Important Dates

Paper submission due: September 30, 2021
Notification of paper acceptance: October 31, 2021
Registration and Final manuscript due: November 15, 2021
Conference: December 13-15, 2021

Special Session Chair

- Dr. Gahangir Hossain, West Texas A&M University, Canyon, Texas

Information Contact: Gahangir Hossain < ghossainATwtamu.edu >