Computers, Materials & Continua

2024 IMPACT FACTOR 1.7

2024 Citescore 6.1 Scopus

Call for Papers

SI: Deep Learning for Next-Generation Cybersecurity: Architectures, Robustness and Applications

Submission Deadline: 15 October 2026
https://www.techscience.com/cmc/special_detail/adversarial-attack

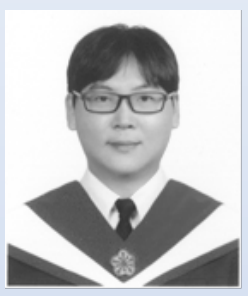
Guest Editors

Prof. Chin-Shiuh Shieh

Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan

Dr. Thanh-Tuan Nguyen

Department of Electronic and Automation Engineering, Nha Trang University, Nha Trang, Vietnam



Dr. Chun-Chih Lo

Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan

Topics

- **Deep Learning architectures for Network Intrusion Detection Systems (NIDS).**
- **Advanced Malware detection and classification using Deep Learning.**
- **Adversarial attacks and defense mechanisms in Deep Learning models.**
- **Privacy-preserving Deep Learning and Federated Learning for security.**
- **Deep Learning-based approaches for IoT and Industrial Control System security.**
- **Generative Adversarial Networks (GANs) for cyber threat intelligence.**
- **Deep Learning for phishing detection and social engineering prevention.**

Summary

In an era of exponential digital interconnectivity, conventional security frameworks increasingly struggle to mitigate the complexities of sophisticated cyber threats. **Deep Learning (DL)** has emerged as a transformative paradigm, offering the self-adaptive and robust capabilities necessary to process massive data streams, identify zero-day vulnerabilities, and automate real-time threat mitigation.

This Special Issue invites cutting-edge research and comprehensive review articles focusing on the intersection of **Deep Learning** and **Cybersecurity**. We seek submissions that address critical challenges in model accuracy, scalability, and resilience against evolving threats. Key areas of interest encompass novel neural architectures for intrusion detection, advanced malware analysis, and privacy-preserving frameworks. Furthermore, we encourage studies on the security of AI itself, specifically regarding adversarial attacks and defense strategies, to provide a holistic perspective on how deep learning can fortify next-generation cyber defense mechanisms.

https://www.techscience.com/journal/cmc
E-mail: cmc@techscience.com

Special Issue