Special Session Proposal
Cybersecurity and Machine Learning: Techniques and Applications

As machine learning (ML) technologies become increasingly integral to a wide array of systems and applications, from autonomous vehicles to financial decision-making tools, the importance of securing these systems against adversarial attacks and ensuring their reliability and safety has never been more critical. This special session is dedicated to advancing the fields of machine learning (ML) and cybersecurity by bringing together the latest research, fostering discussions on emerging challenges and opportunities, and promoting collaborative efforts across academia, industry, and government. Our unified goal is to explore both theoretical approaches and practical implementations that contribute to the development of robust, secure ML systems, showcasing their applications across various domains. Through a comprehensive agenda that includes presenting cutting-edge research, engaging in in-depth discussions on future directions, and highlighting successful case studies, we aim to create a collaborative platform that drives the cybersecurity and ML technologies forward.

Topics of Interest

Submissions are invited on topics related to the security of machine learning, including but not limited to:

- Adversarial machine learning and defense mechanisms
- Privacy-preserving machine learning techniques
- Robustness and generalization in ML models
- Security challenges in deep learning architectures
- Trustworthy and transparent AI systems
- Detection and mitigation of bias in ML algorithms
- Secure federated learning and distributed ML systems
- Applications of secure ML in critical infrastructure, healthcare, finance, and beyond
- Applications of ML in cybersecurity
- ML for anomaly detection systems
- ML in detecting malware in LLM

Submission Guidelines

Prospective authors are invited to submit original, unpublished research papers. Submissions should be formatted according to the conference's guidelines and submitted through the conference submission system. All submissions will undergo a rigorous double-blind peer review process, evaluating them for their originality, technical and/or research content, relevance to the special session theme, and readability.

Important Dates

- Paper Submission Deadline: June 15, 2024
- Notification of Acceptance: June 30, 2024
- Camera-Ready Submission: July 15, 2024
- Special Session Date: [October 4-6, 2024]

Organizing Committee

- Prof. Tarek Gaber, Suez Canal University, Egypt and University of Salford, Manchester, UK, t.m.a.gaber@salford.ac.uk.
- Dr. Mostafa Mohamad, Associate Professor of Digital Transformation and Business Intelligence, Zayed University, College of Interdisciplinary Studies, UAE, mostafa.mohamad@zu.ac.ae.
- Dr. Ahmed Hamed, Assistant Professor, Computer Science Department, Damanhour University, Damanhour, Egypt, ahmed_hamed@cis.dmu.edu.eg.

Special Session on **Cybersecurity and Machine Learning: Techniques and Applications**
Organized at IIHMSP-2024, the 20th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, October 4-6, 2024, Matsue, Japan

- Dr. Mohamed Torky, Assistant Professor, Faculty of Artificial Intelligence, Egyptian Russian University, Cairo, Badr City, 11829, Egypt, Email: mohamed-turki@eru.edu.eg.