*2020 IEEE Applied Imagery Pattern Recognition Workshop*
**Call for Papers**

# AIPR 2020
# *Trusted Computing, Privacy, and Securing Multimedia*

**Cosmos Club, Washington, D.C.**
**October 13-15, 2020**

## Program Chairs:

Prasad Calyam, University of Missouri
Jon Rolf, National Security Agency

## *Call for Paper Abstracts from NSA Centers of Academic Excellence*

Cyber attacks are occurring at unprecedented levels on both legacy and state-of-the-art systems that are vital to our society for media, social interaction, manufacturing, healthcare and energy. Given that attacks are occurring in unexpected ways at different scales, the problem of cyber defense has become an interdisciplinary area that scales across all technologies. Data science, image processing and machine learning based methods are increasingly becoming critical to develop new integrated cloud services to enhance security and privacy of high volume, high value, imaging and multimodal sensor data. There is a need to apply trusted computing techniques in software and hardware associated with applied imagery pattern recognition solutions. Issues with resource constraints as well as human/behavioral aspects create new challenges in increasing the resilience of complex data environments. Further, the rise of social media has created new attack surfaces relating to image/video privacy, veracity, provenance and public perception. Tamper proofing vision, image analysis, AI and machine learning methods will be critical to the adoption of cloud services and ensuring trust in newly emerging autonomous applications. The 2020 IEEE AIPR Workshop will explore these trusted computing applications and multimedia workflows for improving privacy, cybersecurity, trusted social media, resilience of systems for video analytics, and safety of machine learning and autonomous systems.

The Workshop Committee invites papers that address all aspects of how trusted computing can be used to improve cybersecurity, resilience and privacy of multimedia including utilizing robust techniques, methodologies and algorithms from pattern recognition, development of novel tools, and theory and mechanisms of cyber defense operations. Topics include, but are not limited to, the following:

- Cybersecurity & Privacy issues in AI, Autonomy, Pattern Recognition
- Generating Deep Fakes in multimedia (images, video, speech, etc.)

## *2020 IEEE Applied Imagery Pattern Recognition Workshop*
## Call for Papers

- Deep Fake Detection and Characterization / Image Forgery Detection
- Fault-tolerant 3D Computer Vision
- Securing Multimedia Using Block Chains and Related Technologies to Track Computational Cognition and Provenance
- Cyber Defense to protect Image/Video Privacy, Veracity and Provenance
- Visual Steganography
- Privacy and Safety of Biometrics
- Trusted Deep Learning Kernels
- Trusted Hardware Accelerators
- Organically Adaptive Deep Learning for Novel Environments and Situations
- Safe Exploration of Remotely accessible Dynamic Environments
- Remote Sensing and Autonomy
- Securing Human and Robotic Systems
- Visual Edge and Cloud Computing to Process Mobile/IoT Device Data
- Medical Applications, Social Media Applications, etc.
- Election Security and Fake Imagery News Recognition
- Safety and Security of Vision Processing Pipelines in Autonomous Vehicles
- Reinforcement Learning-based Security Mechanisms
- Adversarial Machine Learning Architectures, Formulations, Attack Defense

**Deadline for abstracts: 15 June 2020**. The Workshop will include oral and poster presentations, several keynote talks that provide in-depth overviews of the fields, and a special session on the theme topic. Written papers will be required (due after the workshop) and will be indexed in IEEEXplore. AIPR 2020, the 49th annual workshop, is sponsored by the IEEE Computer Society Technical Committee on Pattern Analysis and Machine Intelligence, and organized by the AIPR Workshop Committee with generous support from other sponsors. Updates and additional information can be found at www.aipr-workshop.org.