IEEE International Conference on Assured Autonomy (ICAA)

CALL FOR PAPERS

https://iaa.jhu.edu/icaa/

Important Dates

- Paper submission deadline: 11/08/2021 (Anywhere on Earth)
- Acceptance notification: 12/06/2021
- Publication-ready Papers Due: 01/06/2022
- Conference: March 22 – 24, 2022, Puerto Rico (Hybrid)

Overview

The IEEE International Conference on Assured Autonomy (ICAA) plans to address the gap that exists between theory-heavy autonomous systems and algorithms and the privacy, security, and safety of their real-world implementations. Advances in machine learning and artificial intelligence have shown great promise in automating complex decision-making processes across transportation, critical infrastructure, and cyber infrastructure domains. Practical implementations of these algorithms require significant systems engineering and integration support, especially as they integrate with the physical world. This integration is wrought with artificial intelligence (AI) safety, security, and privacy issues.

The primary focus of this conference is the: (1) detection of, (2) response to, and (3) recovery from AI safety, security, and privacy violations in autonomous systems. Key technical challenges include discriminating between application-layer data breaches and benign process noises, responding to breaches and failures in real-time systems, and recovering from decision making failures autonomously.

Topics of Interest

ICAA seeks contributions on all aspects of AI safety, security, and privacy in autonomous systems. Papers that encourage the discussion and exchange of experimental and theoretical results, novel designs, and works in progress are preferred. Topics of interest include (but are not limited to):

Autonomous System and AI Safety

- Detecting dataset anomalies that lead to unsafe AI decisions
- Evaluating safety of autonomous systems according to their potential risks and vulnerabilities
- Resilient, explainable deep learning, and interpretable machine learning
- Verification, testing and acceptance of machine learning models and autonomous systems

- Autonomic computing for autonomous system safety
- Standards, ethics, and policies for autonomy and AI safety
- Ethics of autonomous system behaviors, algorithms and implementations
- Safety and assurance of human-autonomy teaming

Security and Privacy of Autonomous Systems and AI

- Detecting dataset anomalies that lead to autonomous system security and privacy violations
- Differential privacy and privacy-preserving learning and generative models
- Adversarial attacks on AI and autonomy, and defenses against adversarial attacks
- Improving resiliency of AI and autonomous system methods and algorithms to various forms of attacks
- Engineering trusted autonomous system and AI software architectures

Submission Guidelines

You are invited to submit regular papers of up to ten pages, or four pages for works-in-progress, including references. To be considered, papers must be received by the submission deadline. Submissions must be original work and may not be under submission to another venue at the time of review. Please mark all of your conflicts of interest when submitting your paper. Papers should be in IEEE conference format. Templates can be found at https://www.ieee.org/conferences/publishing/templates.html.

Presentation Form

All accepted submissions will be presented at the conference and included in the IEEE conference proceedings. Due to time constraints, accepted papers will be selected for presentation as either talk or poster based on their review score and novelty. Nonetheless, all accepted papers should be considered as having equal importance.

One author of each accepted paper is required to attend the conference and present the paper for it to be included in the proceedings.

Submission Web Site

https://iaa.jhu.edu/icaa/