Workshop on Recent Advances in Resilient and Trustworthy MAchine learning-driveN systems (ARTMAN 2024)

The 2^{nd} Workshop on Recent Advances in Resilient and Trustworthy MAchine learning-driveN systems (ARTMAN) will be held on Monday, December 9^{th}, 2024, in conjunction with the Annual Computer Security Applications Conference (ACSAC). ACSAC will be held in Waikiki, Hawaii.

Call for Papers. This workshop aims at bringing together academic researchers and industrial practitioners from different domains with diverse expertise (mainly security & privacy and machine learning, but also from application domains) to collectively explore and discuss the topics about resilient and trustworthy machine learning-powered applications and systems, share their views, experiences, and lessons learned, and provide their insights and perspectives, so as to converge on a systematic approach to securing them. One of the ultimate objectives, which deserves a series of multiple workshops to achieve, is to foster the close collaboration between researchers and practitioners to improve the security, privacy, and trust of ML applications in a series of heterogeneous and complex systems, such as cyber-physical systems and intelligent manufacturing systems. On the one hand, it is important for academic researchers to practically specify threat models in terms of attacker intent, objectives, skills (knowledge, capabilities), and strategies (by taking into account cost factors). For example, an attacker may employ a simple yet effective data poisoning method instead of gradient computations to evade ML-based anomaly detection systems. On the other hand, the practitioners should be strongly encouraged to share their observations and insights during the development and deployment of production-grade AI systems (generally called intelligent systems), most of which are invisible or closed. This can help academics understand how real-life AI systems normally work and set up more realistic assumptions to develop ML security research and address real-world concerns. The results and impacts of this workshop are expected to go beyond the research community, hopefully providing valuable findings and recommendations to the telecommunications stakeholders, standards-developing organizations, and government sectors.

Without enforcing strong limitations on the use cases in which AI/ML systems may be deployed, we encourage contributions and discussions both foundational to ML systems and applied, with specific interest in self-driven networks, digital twins, large language models, and healthcare AI. This workshop is also interested in soliciting contributions on applying AI/ML algorithms, especially those knowledge-informed ones, to improve resilience and trust in such scenarios.

Topics of Interest. This workshop will be focused on the **resilience** and **trustworthiness** of machine learning-driven systems. Resilience refers to the ability of an AI/ML system to maintain required capability and expected performance in the face of adversity, covering both dependability (accidental failures) and security (intentional attacks) issues. Trustworthiness refers to the attribute that an AI/ML system provides confidence to users of their capabilities and reliability in performing given tasks. Their overlap lies in the core interests of the dependability community. More specifically, this workshop is intended to cover the following topics, with slight extension if necessary,

- **Threat modeling and risk assessment** of ML systems and applications in intelligent systems, including, but not limited to, anomaly detection, failure prediction, root cause analysis, incident diagnosis
- **Data-centric attacks and defenses** of ML systems and applications in intelligent systems, such as model evasion via targeted perturbations in testing samples, data poisoning in training examples
- **Adversarial machine learning**, including adversarial examples of input data and adversarial learning algorithms developed for intelligent systems
- **ML robustness**: testing, simulation, verification, validation, and certification of the robustness of ML pipelines (not only ML algorithms and models) in intelligent systems, including but not limited to data-centric analytics, model-driven methods, and hybrid methods
- **AI system safety**: dependability topics related to AI system development and deployment environments, including hardware, ML platform and framework, software

- **Trust in AI systems and applications**: this mainly explores the trust issues arising from the interactions between human users and AI systems (e.g., Man-Machine Symbiosis, Human-Machine Teaming), with a particular focus on interpretable, explainable, accountable, transparent, and fair AI systems and applications in intelligent systems
- **Resilience by reaction**: leveraging AI/ML algorithms, especially knowledge-informed models, to improve resilience and trust of intelligent systems

---

Submission Guidelines

Submissions should be 6 to 10 pages excluding references and appendices, using double-column IEEE template available here with `\documentclass[conference,compsoc]{IEEEtran}`. 5 additional pages can be used for references and well-referenced appendices. Note that the reviewers are not expected to read these appendices.
The submission website is: `https://easychair.org/conferences/?conf=artman2024`
All submissions must be anonymous, i.e., author names and affiliations should not be included. Authors can cite their work but must do so in the third person.
Accepted workshop papers will be published by IEEE Computer Society Conference Publishing Services (CPS), see below.

Publication

Accepted papers will be published by IEEE Computer Society Conference Publishing Services (CPS) and will appear in the Computer Society Digital Library and IEEE Xplore® in an ACSAC Workshops 2024 volume alongside the main ACSAC 2024 proceedings.

ACSAC is currently transitioning to technical sponsorship by IEEE Computer Society's Technical Community on Security and Privacy (TCSP) and expect approval before the proceedings are compiled.

Important Dates

Submission Deadline September 15, 2024

Acceptance Notification October 20, 2024

Camera Ready Deadline November 1, 2024

Workshop Date December 9, 2024

Visa Request for Workshop Participants

ACSAC is being held in the US, so participants from outside the US may require a visa to travel to the conference and workshops. Since the US visa process varies based on nationality, we would like to inform any author submitting work to ARTMAN to request a visa letter in advance by following the instructions found here.

Authors outside the US should apply for a visa letter in anticipation of their work being accepted. However, the visa letter does not indicate that their work will be accepted in the workshop. It is to remediate the potential delay and last-minute requests that can impact their travel plans. We also encourage the organizers to make a decision on accepting papers as soon as possible to give authors requiring a visa to the US time to process one.

Program Committee

Workshop Co-chairs

Gregory Blanc, Telecom SudParis, Institut Polytechnique de Paris, France

Takeshi Takahashi, National Institute of Information and Communications Technology, Japan

Zonghua Zhang, CRSC R&D Institute Group Co. Ltd., China

Program Committee Members

Muhamad Erza Aminanto, Monash University, Indonesia

Laurent Bobelin, INSA Centre Val de Loire, France

Sajjad Dadkhah, University of New Brunswick, Canada

Doudou Fall, Ecole Supérieure Polytechnique, Cheikh Anta Diop University, Senegal

Joaquin Garcia-Alfaro, Telecom SudParis, Institut Polytechnique de Paris, France

Pierre-François Gimenez, CentraleSupélec, France

Yufei Han, Inria, France

Frédéric Majorczyk, DGA, France

Ikuya Morikawa, Fujitsu, Japan

Antonio Muñoz, University of Malaga, Spain

Mehran Alidoost Nia, Shahid Beheshti University, Iran

Misbah Razzaq, INRAE, France

Balachandra Shanabhag, Cohesity, USA

Toshiki Shibahara, NTT, Japan

Pierre-Martin Tardif, Université de Sherbrooke, Canada

Fredrik Warg, RISE Research Institutes of Sweden

Akira Yamada, Kobe University, Japan

Workshop Registration

If you are interesting in attending, please check off the appropriate box on the conference registration form and add in the ARTMAN Workshop fee. For accepted papers, at least one author must register and attend.
Further details about the workshop can be found either on the workshop website (`https://artman-workshop.gitlab.io/`) or by contacting the organizers at `artman2024@easychair.org`.