IEEE CONSUMER ELECTRONICS MAGAZINE
- SPECIAL ISSUE CALL FOR ARTICLES -

Adversarial Examples in CE: Deceptive Threats to AI Systems

Artificial Intelligence (AI) has found extensive applications in various domains of Consumer Electronics (CE), including FinTech, smart homes, autonomous driving, information security, and so on. It encompasses various data types such as voice, Natural Language Processing (NLP), images, videos, wireless radio-frequency signals, and more. AI excels in feature extraction, prediction, and recognition across these diverse data types. In essence, humanity has become inseparable from AI. In this context, attackers have shifted their focus to the core of AI, creating Adversarial Examples (ADV) that escape human perception with the intention of deceiving AI models. These versatile ADVs can be concealed within various data types. The development of such attacks poses a significant threat to humanity, particularly in a scenario where our dependence on AI continues to grow. By delving into ADV attack techniques, prevention methods, and mitigation strategies in the realm of CEs, this special issue aims to provide valuable insights and knowledge for *IEEE Consumer Electronics Magazine* readers.

TOPICS OF INTEREST

This special issue is dedicated to AI security and privacy of CE hardware and software systems. We welcome submissions on various aspects, including attacks design, predictions, and preventive measures related to ADVs in CE across different domains. Topics of interest include but are not limited to:

- ADV attacks and defenses in reinforcement learning or federated learning
- Advancements in ADV techniques using various AI/ML and metaheuristic algorithms
- Adversarial training techniques in AI-SPC
- ADVs in fake news detection
- Exploring explainable AI (XAI) in the context of ADVs
- Identification of counterfeit radio-frequency base stations based on ADVs
- Identification and defense against ADVs in biometric payment systems (e.g., fingerprint, voiceprint, facial recognition) within FinTech CE
- Impact of ADVs on autonomous driving safety and mitigation strategies
- Novel ADV attack designs in the AI-SPC domain
- Value-added applications of ADV-related research in various CE domains

AUTHOR GUIDELINES

IEEE Consumer Electronics Magazine (CEM) publishes peer-reviewed articles that present emerging trends, key insights, tutorials, practical experiences, design, and industry-related research & developments of mainstream consumer electronic products, technologies, and related fields of interest to the membership of the IEEE Consumer Technology Society (CTSoc) and broad engineering audience. CEM aims to educate and entertain on general topics related to consumer technologies and electronic products.

Submissions must follow IEEE CEM Template available in IEEE Template Selector[1], or the LaTeX template is also available on Overleaf[2], and should consist of the followings: (i) A manuscript of minimum 6-page length (overlength page charges are listed below): A PDF of the complete manuscript layout with figures, tables placed within the text, and (ii) Source files: Text should be provided separately from photos and graphics and may be in LaTeX or Word format. High-resolution original photos and graphics (300 dpi) are required for the final submission. Images embedded in Word or Excel documents are not suitable; however, figures and graphics may be provided in a PowerPoint slide deck, with one figure/graphic per slide.

The authors must own the copyright on any images, photographs or graphics or have obtained explicit permission for use of all such material when a third party owns the copyright. Alternatively, copyleft images and materials may be used once the relevant license terms are complied with, including citations to the original source/author. It is the responsibility of the author(s) to demonstrate such compliance and document the corresponding license agreements (a URL is sufficient) in notes accompanying the submitted article. The authors should include a PDF file with a suggested layout of the article. Figure captions must be provided and ideally figures/graphics should be cited in the text of the article. An IEEE copyright form will be required.

The manuscripts must be submitted online to the *'Special Issue on Adversarial Examples in CE: Deceptive Threats to AI Systems'* track using the IEEE CEM's IEEE Author Portal[3]. The IEEE Author Portal will automate the generation of a single submission document if the authors have the correct files prepared in advance.

OVERLENGTH PAGE CHARGES

Articles exceeding 6 pages during author proof will be charged at US$ 250 per page for extra pages beyond first allowed 6 pages.

IMPORTANT DATES

- *ARTICLE SUBMISSION DUE:* April 1, 2024
- *FIRST ACCEPTANCE NOTIFICATION:* August 1, 2024
- *FINAL ACCEPTANCE NOTIFICATION:* November 1, 2024
- *APPROX. PUBLICATION DATE IN PRINT:* Q3 2025

GUEST EDITORS

- Chia-Mu Yu, National Yang Ming Chiao Tung University, Taiwan (Lead Guest Editor; chiamuyu@gmail.com)
- Hsin-Hung Cho, National Ilan University, Taiwan (hhcho@niu.edu.tw)
- Reza Malekian, Malmö University, Sweden (reza.malekian@ieee.org)
- Alireza Jolfaei, Flinders University, Australia (alireza.jolfaei@flinders.edu.au)
- Lei Shu, Nanjing Agricultural University, China/University of Lincoln, UK (lei.shu@njau.edu.cn)

[1] IEEE Template Selector: https://template-selector.ieee.org/
[2] LaTeX Template at Overleaf: https://www.overleaf.com/latex/templates/ieee-consumer-electronics-magazine-template/xphtjrbwmvrz/
[3] IEEE Author Portal: https://ieee.atyponrex.com/journal/cemag/

@ieeectsoc
www.ctsoc.ieee.org
IEEE CTSoc CONSUMER TECHNOLOGY SOCIETY
v231115