ICICLE
DEMOCRATIZING AI

NEWSLETTER

ISSUE 7 - MARCH 2023

Upcoming Event

THURSDAY, MARCH 30, 2023 AT 10:30 AM ET

**ALFONSO MORALES,
VILAS DISTINGUISHED ACHIEVEMENT
PROFESSOR CHAIR, TO PRESENT**

“OPPORTUNITIES AND NEEDS IN AI AND CI FOR DIRECT MARKETING FARMING AND FARMERS MARKETS”

**AT
AI FOR SOCIAL IMPACT SEMINAR SERIES
[FLYER]**

Welcome

Edna Ely-Ledesma (UW)
Yuxiao Qu (UW)

Say Hi to our New Members !

Team Spotlight

Abdullah Caglar Oksuz, presented at the NDSS Symposium 2023,a leading security forum that fosters information exchange among researchers and practitioners of network and distributed system security.
Model extraction attack is one of the most prominent adversarial techniques to target machine learning models along with membership inference attack and model inversion attack. Capabilities of adversarial ML attacks can be enhanced by combining the additional vulnerabilities Explainable Artificial Intelligence (XAI) produces. The poster demonstrates using novel model extraction attack called AUTOLYCUS against decision-tree models. Poster details can be found here

Abdullah Caglar Oksuz, Anisa Halimi , Erman Ayday, “AUTOLYCUS: Exploiting Explainable AI (XAI) for Model Extraction Attacks against Decision Tree Models” , Network and Distributed System Security Symposium (NDSS), March 2023

ICICLE
DEMOCRATIZING AI

ICICLE AI INSTITUTE EDUCATIONAL FELLOWSHIP PROGRAM: INAUGURAL THEME OF DEMOCRATIZING AI

The Intelligent Cyberinfrastructure with Computational Learning in the Environment (ICICLE) Artificial Intelligence (AI) Institute's launched its Educational Fellowship program. The goal of the program is to engage graduate students, postdoctoral fellows, and early-career educators and researchers in career building experiences and opportunities at the nexus of artificial intelligence, cyberinfrastructure, and education and training while furthering the educational and outreach objectives of the institute. The 2023 program theme is Democratizing AI: making AI more accessible to a wider range of potential users, engaging a wide range of people in the design of AI, and democratizing the benefits of AI. The successful ICICLE Educational Fellow engages with the ICICLE institute through a nine-month fellowship. The activities of the fellow can be inspired by any of ICICLE's working groups and thrust areas, including intelligent cyberinfrastructure; privacy, accountability, and data integrity; AI ethics and democratization; smart foodsheds; animal ecology; and AI literacy.

Additional details can be found here . Questions, please contact pti@iu.edu.

ICICLE'S TIPS ON ALLYSHIP

The Broader Impact Backbone Network team sends out tips in video format on how we, here at ICICLE, can become better allies

TO PROMOTE AN AWARE , INCLUSIVE , AND MORE DIVERSE COMMUNITY

Browse all Tips for Allyship here

RECENT PRESENTATIONS & PUBLICATIONS

PRESENTATIONS

- Rajiv Ramnath, "Designing Next-Generation Intelligent Cyber-Infrastructure: ICICLE NSF-AI Institute", SAGE/MSRI/AI Institute Workshop on Developing a Vision for AI-Enabling Cyberinfrastructure, March 2023
- Abdullah Caglar Oksuz, Anisa Halimi , Erman Ayday, "AUTOLYCUS: Exploiting Explainable AI (XAI) for Model Extraction Attacks against Decision Tree Models" , Network and Distributed System Security Symposium (NDSS), March 2023

PUBLICATIONS

- A Reflection on AI Model Selection for Digital Agriculture Image Datasets, Seth Ockerman, John Wu, Christopher Stewart, Zichen Zhang, January 2023 Workshop on AI for Agriculture and Food Systems
- E Romero-Gainza, C Stewart, "AI-Driven Validation of Digital Agriculture Models" In: MDPI Sensors 23 (3), January 2023

Click **here** to view ICICLE Presentations and Publications

ICICLE
DEMOCRATIZING AI

COMING SOON

ICICLE NEXTGENS ONLINE COMMUNITY NETWORK

ICICLE will soon launch an online community network "ICICLE Next Generation (NextGens)" open to all ICICLE students (High School, Undergraduate, Graduate, PhD) to help them stay connected and represents what they are as professionals in our organization. Stay tuned !

Questions, please contact Maureen Biggers

JOIN OUR MAILING LISTS !

The following mailing lists are available for ICICLE software and cyberinfrasturucture releases, future updates and miscellaneous questions regarding installation/build problems, performance issues.

- **icicle-announce**: This is an announcement list only. If you would like to get information about future updates, software and cyberinfrastructure releases, publications, etc. related to the ICICLE project, you may subscribe to this mailing list. This list is open to public. You are welcome to subscribe to this mailing list yourself.

- **icicle-discuss**: This is a discussion list. This mailing list is meant for users to discuss all installation/build problems, performance issues , features and other miscellaneous questions related to the different software and cyberinfrasturucture components of the ICICLE project. In order to post your questions and suggestions to this mailing list, you need to be a registered user of ICICLE with an organizational e-mail address and be a member of this list by subscribing to it with the same e-mail address. If you are not a registered user, please follow the procedure indicated under Download tab in the top menu to get registered.

We welcome your interest to partner with ICICLE! Please complete this **form** and we'll reach out to you.

Follow us @icicleai

NEWSLETTER

Newsletter Archives

Subscribe