Yuechun Gu

Details

(414) 285-8673
ethan.gu@marquette.edu

Links

linkedin

Personal page

Skills

Keras (Neural Network Library)

C (Programming Language)

Python (Programming Language)

PyTorch (Machine Learning Library)

Tensorflow

Languages

English

Mandarin

Profile

I'm a Ph.D. student at Marquette University. I'm interested in privacy and confidentiality in machine learning, applied machine learning, computer vision, and machine learning in biology.

Employment History

Research Assistant, Marquette University Milwaukee, Milwaukee

JANUARY 2021 – PRESENT

Collaborating with Dr. Keke Chen, we've published three papers on dataset encoding and inference attacks, contributing to conferences and journals like AAAI, CCS, and ACM TOIT. Our latest work includes a paper on adaptive inference attacks submitted to IEEE S&P and ongoing research on privacy budget implications in differential privacy.

Systems Specialist, EF Education First, Tianjin

JUNE 2020 – JANUARY 2021

Developed a Salesforce-based database warehouse for EF Tianjin.

Research Assistant, UCLA, Los Angeles

JUNE 2018 – JANUARY 2020

Collaborated with Dr. Da Yan and Dr. Sibo Yan to implement an LSTM-based regression algorithm that significantly improved the predictive accuracy of high-frequency stock price models.

Education

Doctorate Computer Science, Marquette University, Milwaukee

JANUARY 2021 – PRESENT

Bachelor of Science in Mathematics, University of Electronic Science and Technology of China

AUGUST 2016 – JUNE 2020

Reasearch and Publications

Privacy budget implications in differential privacy

JULY 2023 – PRESENT

Conducting research on a novel approach to understanding privacy budgets, targeting submission to CCS'24.

Image Disguising for Scalable GPU-accelerated Confidential Deep Learning

JANUARY 2023 – JULY 2023

Designed a GPU-accelerated dataset encoding platform utilizing AES, RMT, and NeuraCrypt, accepted for presentation at CCS'23.

[Paper] [github]

Adaptive Domain Inference Attack

JULY 2022 – DECEMBER 2023

Addressing the challenge of attackers knowing data domains in inference and inversion attacks, we crafted an efficient domain inference attack utilizing an adaptive, tree-like architecture. Submitted to IEEE S&P.

[Preprint]

DisguisedNets: Secure Image Outsourcing for Confidential Model Training in Clouds

JANUARY 2022 — JANUARY 2023

We propose DisguisedNets, an image disguising method for secure cloud-based training of deep neural networks (DNNs), circumventing the high costs, inefficient GPU utilization, and client-side processing burdens of current cryptographic solutions. Accepted by ACM TOIT.

[Paper]

GAN-based domain inference attack

DECEMBER 2021 — OCTOBER 2022

Developed a novel GAN-based Model Domain Inference (MDI) attack method to identify likely domains of a target classification model without prior domain knowledge, enhancing the effectiveness of model-inversion attacks.

[Paper]

Price forecast with high-frequency finance data: An autoregressive recurrent neural network model with technical indicators

JUNE 2019 — JANUARY 2020

Explored intraday forecast of price patterns using high-frequency trade data, demonstrating that autoregressive recurrent networks with technical indicators as covariates outperform traditional LSTM models and GARCH, commonly used in finance. Accepted by CIKM.

[Paper]