Yuxuan Zhu

+1 5189619609 zhuy27@rpi.edu Google Scholar linkedin Homepage

Education

Rensselaer Polytechnic Institute (RPI) **Aug. 2023 – Now**
***Ph.D** in Computer Science* *Troy, New York, USA*

Leiden University **Feb. 2021 – Mar. 2023**
***Master of Science** in Computer Science* *Leiden, Netherlands*

Sichuan University **Sept. 2016 – June 2020**
***Bachelor of Engineering** in Medical Information Engineering* *Chengdu, China*

Research Interest

Efficient LLM, KV Cache Compression, Trustworthy AI, Anomaly Detection, Graph Neural Network

Publications

Zhu, Y etc. SentenceKV: Efficient LLM Inference via Sentence-Level Semantic KV Caching
In preparation.

Zhu, Y etc. On the Robustness of Graph Reduction Against GNN Backdoor.
Proceedings of the 2024 Workshop on Artificial Intelligence and Security.
https://arxiv.org/abs/2407.02431

Li, Z, **Zhu, Y** & van Leeuwen, M A Survey on Explainable Anomaly Detection.
ACM Transactions on Knowledge Discovery from Data (TKDD) - Top 5 downloaded papers.
https://doi.org/10.1145/3609333

Research Experience

Research Assistant, Amiri Lab **Sept. 2024 – Now**
Advisors: Mohammad Mohammadi Amiri (Assistant Professor) *Troy, USA*

- Research **efficient KV caching** for LLMs to improve memory usage, and preserve contextual information, especially for long-context scenarios. My work introduces a sentence-level semantic caching mechanism that reduces redundancy while preserving model performance.

Research Assistant, Data Security and Privacy Lab **Aug. 2023 – Aug. 2024**
Advisors: Lei Yu (Assistant Professor) *Troy, USA*

- Research the scalability challenges and security concerns, specifically backdoor poisoning attacks, faced by Graph Neural Networks (GNNs) when applied to large-scale graph data.
- Research the training data leakage problem (which is called Membership Inference Attack) on LLMs

Research Assistant, Explanatory Data Analysis group **Nov. 2021 – Sept. 2022**
Advisors: Matthijs van Leeuwen (Associate Professor), Zhong Li (PhD candidate) *Leiden, Netherlands*

- Proposed framework(s) to unify existing interpretable anomaly detection methods
- Perform comparative evaluations and apply some typical techniques to real-world use cases.

Research Assistant, Lab of Super-Resolution Imaging **Oct. 2018 – July 2019**
Advisor: Han Zhang (Associate Professor) *Chengdu, China*

- Proposed a method, completed proofs of a nonlinear two-photon structured illumination microscopy

Work Experience

Research Intern, Inkjet Failures Detection and Classification **Sept. 2022 – Mar. 2023**
Advisors: Fatima Abidine, Matthijs van Leeuwen *Canon NL, Netherlands*

- The project is part of the Digital Twin program funded by Dutch Research Council (NWO)
- Identified and clustered anomalies using industrial time-series data.
- Labeled and mapped outlier clusters with expert knowledge.
- Visualized results and provided suggestions to enhance Canon's inkjet failure detection methods.

Skills

PyTorch, Python, C++, Matlab