

Alexander Nemecek

alex.nemecek@att.net | (216) 501-3231 | [LinkedIn](#) | [Personal Site](#)

EDUCATION

Case Western Reserve University – Cleveland, OH

Aug 2023 – Expected May 2027

Ph.D. Candidate, Computer Science

Focus: Watermarking in Large Language Models (LLMs), AI Governance

Ohio University – Athens, OH

Aug 2019 – May 2023

B.S., Computer Science – B.S., Psychology

TECHNICAL SKILLS

Languages: Python, C/C++, JavaScript, TypeScript, SQL, Bash

AI/ML: PyTorch, TensorFlow, Hugging Face Transformers, LangChain

Tools & Platforms: AWS, Git, Linux, React Native, Slurm, Snowflake, Tableau

Data Analysis: Pandas, NumPy

EXPERIENCE

Case Western Reserve University – Cleveland, OH

Aug 2023 – Present

Graduate Researcher

- Developed semantic-aware **watermarking** scheme for **LLMs** using topic-aligned token partitioning in **PyTorch**, maintaining text quality at industry-leading levels and increasing adversarial robustness by 30%.
- Directed cross-disciplinary **AI Governance** analysis, designing a three-layer policy-technical framework adopted to align regulatory expectations with watermarking capabilities.
- Engineered and deployed end-to-end **AI** stress detection platform (**AWS Lambda**, **Fitbit API**, **React**) with personalized models; led an **Agile** team of 10 junior engineers.

Sandia National Laboratories – Albuquerque, NM

May 2024 – Present

Research and Development Intern

- Built real-time threat detection pipeline leveraging fine-tuned **LLMs** with **LoRA** in **PyTorch**, improving model accuracy by 18% and enabling production deployment.
- Implemented adaptive **LoRA fine-tuning** infrastructure for dynamic model swapping, speeding up knowledge graph extraction workflows.
- Designed a prompt engineering framework with semantic guardrails; adopted by security teams for strategic threat prioritization.

Cisco Systems – Richfield, OH

May 2023 – Aug 2023

Software Engineer Intern

- Rebuilt full-stack BOM analysis platform (**Python**, **Snowflake**, **React**), automating manual processes into user-friendly application and transforming hardware engineering workflows from error-prone to efficient.
- Developed **Python** data pipeline standardizing vendor BOM formatting into **Snowflake** warehouse with integrated **SQL** pipelines, reducing analysis time by 60%.
- Created interactive pricing trend visualizations in **React** that accelerated procurement decision cycles from three months to one month across cross-functional teams.

Sherwin-Williams – Cleveland, OH

May 2022 – Aug 2022

Software Engineer Intern

- Constructed **SQL** and **Snowflake** pipelines to centralize nationwide automotive paint data, improving accessibility and operational efficiency.
- Designed **Tableau** analytics platform visualizing 20+ KPIs, resolving data inconsistencies to improve inventory management and sales forecasting decisions.

Ohio University – Athens, OH

Sep 2021 – Mar 2023

Student Researcher

- Implemented secure cross-platform mobile app for foster care memory preservation with **AWS** backend storage and privacy-compliant architecture, implementing **CI/CD** pipeline with automated testing.
- Developed **VR/AR** control interfaces for industrial robotics using **Meta Quest** and **HoloLens**, improving remote worker safety operations.

PUBLICATIONS & PREPRINTS

- A. Nemecek**, Y. Jiang, E. Ayday, “The Feasibility of Topic-Based Watermarking on Academic Peer Reviews,” [IJCNLP-AACL](#), December 2025.
- M. Namazi, **A. Nemecek**, E. Ayday, “ZKPROV: A Zero-Knowledge Approach to Dataset Provenance for Large Language Models,” [arXiv](#), June 2025.

- **A. Nemecek**, Y. Jiang, E. Ayday, “Watermarking Without Standards Is Not AI Governance,” [*ICML Technical AI Governance \(TAIG\) Workshop*](#), May 2025.
- **A. Nemecek**, E. Yilmaz, E. Ayday, “Cluster-Aware Attacks on Graph Watermarks,” [*arXiv*](#), Apr 2025.
- **A. Nemecek**, Y. Jiang, E. Ayday, “Topic-Based Watermarks for Large Language Models,” [*arXiv*](#), Fed 2025.

PRESENTATIONS

- **A. Nemecek**, R. Abbott, C. Garasi, “Can Smaller Expert Modules Enhance RAG Performance?,” [*Chesapeake Large-Scale Analytics Conference \(CLSAC\)*](#), Nov 2024.
- **A. Nemecek**, Y. Jiang, E. Ayday, “Topic-Based Watermarks for Large Language Models,” [*Privacy Enhancing Technologies Symposium \(PETS\)*](#), July 2024.
- **A. Nemecek**, C. Mourning, “Detection of Network Attacks using Machine Learning Models,” [*The Ohio Journal of Science*](#), Apr 2023.