HARI PRIYA MUPPIDI

Experienced Software Engineer specializing in scalable system architecture and end-to-end solutions.

Projects

Privacy-Preserving Optimizers for Image Classification

- Achieved 65% accuracy on CIFAR-10 under strict privacy guarantees ($\varepsilon=3.0$, $\delta=10^{-5}$) by implementing grouped gradient clipping, adaptive learning rates, and per-layer noise scaling in optimizers like SGD, RMSprop, and AdaGrad.
- Reduced training time by 10% using weight standardization and parameter averaging techniques.
- Delivered a scalable privacy-preserving framework for image classification, enabling robust machine learning in sensitive data scenarios.

Privacy-Preserving Machine Learning for Customer Churn Prediction

- Developed a differentially private logistic regression model using gradient clipping on the Telco Customer Churn dataset, achieving 80% accuracy with privacy guarantees.
- Generated synthetic datasets with 90% feature utility retention using the Laplace mechanism for noisy histograms.
- Optimized different hyperparameters, including batch size, clipping threshold, and sigma to balance privacy and performance.

Red teaming LLM Agents

- Investigated vulnerabilities in Large Language Model (LLM)-based agents, specifically targeting Cactus (chemical property analysis) and PaperQA (document evidence retrieval).
- Evaluated the robustness of these agents against prompt injection attacks, highlighting potential security risks associated with their instruction-following tendencies.

Work Experience

Accenture (Infrastructure Management - Middleware team for Ross Stores)

Custom Software Engineering Analyst (August 2021 – July 2023)

- Applied WebLogic and Log4j vulnerability patch updates across 100+ middleware instances in production and non-production environments.
- Tested automated scripts to streamline security patch updates reducing downtime.
- Resolved 50+ backup failures and monitored alerts for 200+ application environments, ensuring consistent performance of the instances.

Contact

Phone: 404-558-9263
Email: haripriyamuppidi02@gmail.com
www.linkedin.com/in/hari-priya-muppidi-9a5809336

Educational Background

Master of Science, Computer Science, University of Georgia
(Aug 2023 - May 2025)

- GPA : 3.6 / 4.0
- Coursework : Privacy-preserving data analysis, Red-teaming Large Language Models(LLMs), Algorithms, Computer Networks, Database Management, Software Engineering

Technical Skills

Languages/Frameworks

- Python
- C++
- Java
- Javascript, React
- HTML,CSS
- Typescript
- Flask
- PHP

Tools/Sofware

- Git
- Google Colab
- Opacus

Certifications

- Introduction to Databases - Meta
- Google Cloud Computing Foundations

ON CAMPUS INVOLVEMENTS

Teaching Assistant –Spring 2024

Graded 4 sections for CSCI 2670 - Theory of Computing course.

Security Student Assistant - Fall 2023

Regulated and ensured the compliance and safety for 1 00+ students.