Evan Sage

Department of Computer Sciences
University of Wisconsin-Madison
1210 W Dayton St, Madison, WI 53706
Email: evan.sage@wisc.edu
Website: evan-sage.github.io

Education

- **Ph.D. in Computer Sciences**, University of Wisconsin-Madison August 2021 - Present
  Advisor: Prof. Lisa Thompson
  Research Focus: Safe and robust artificial intelligence, adversarial machine learning.
- **B.S. in Computer Science**, Massachusetts Institute of Technology (MIT) September 2017 - June 2021
  Minor: Mathematics
  Graduated with honors (GPA: 4.0/4.0)
  Thesis: *Enhancing Neural Network Robustness Against Adversarial Attacks*

Research Interests

Safe and robust artificial intelligence; adversarial machine learning; secure multi-agent systems; ethics and fairness in AI; machine learning security protocols.

Publications

1. **E. Sage**, L. Thompson, "Adversarial Resilience in Deep Learning Models," *Proceedings of the 2023 Conference on Neural Information Processing Systems (NeurIPS)*, 2023.
2. **E. Sage**, "Ethical Considerations in Multi-Agent AI Systems," *Journal of AI Ethics*, vol. 15, no. 2, pp. 123-134, 2022.
3. **E. Sage**, L. Thompson, "Secure Protocols for Multi-Agent Communication," *International Conference on Machine Learning (ICML)*, 2022.
4. **E. Sage**, M. Patel, "Defensive Strategies Against Adversarial Examples," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 10, pp. 4567-4578, 2021.

Teaching Experience

Teaching Assistant, University of Wisconsin-Madison

- **CS 540: Introduction to Artificial Intelligence** Fall 2023
  Responsibilities: Led discussion sections, held office hours, graded assignments and exams.

- **CS 577: Introduction to Algorithms** Spring 2023
  Responsibilities: Assisted in preparing lecture materials, held recitation sessions, provided student support.

Guest Lecturer

- "Adversarial Machine Learning" in **CS 760: Machine Learning** November 2023
  Covered topics on adversarial attacks and defenses in machine learning models.

Research Experience

Graduate Researcher, University of Wisconsin-Madison August 2021 - Present

- Developing robust neural networks capable of withstanding adversarial attacks.
- Investigating secure communication protocols in multi-agent AI systems.

Undergraduate Research Assistant, MIT CSAIL September 2019 - June 2021

- Conducted research on enhancing the robustness of machine learning models.
- Assisted in projects related to AI ethics and fairness under Prof. Maria Rodriguez.

Awards and Honors

- **Best Student Paper Award**, AI Ethics Conference 2023
  For the paper "Ethical Considerations in Multi-Agent AI Systems."
- **UW-Madison Graduate Research Fellowship** 2022
  Awarded for outstanding research potential in the field of computer sciences.
- **MIT Dean's List** 2017 - 2021
  Recognized for academic excellence each semester.

Professional Activities

Reviewer

- *Neural Information Processing Systems (NeurIPS) Conference* 2023
- *Journal of Machine Learning Research (JMLR)* 2022 - Present

Member

- Association for Computing Machinery (ACM)
- IEEE Computer Society

Technical Skills

- **Programming Languages:** Python, Java, C++, MATLAB, R
- **Machine Learning Frameworks:** TensorFlow, PyTorch, Scikit-learn
- **Tools and Platforms:** Git, Docker, Linux, AWS

Selected Presentations

- "Adversarial Resilience in Deep Learning Models," NeurIPS Conference December 2023
- "Secure Protocols for Multi-Agent Communication," ICML Conference July 2022
- "Enhancing Neural Network Robustness," MIT Undergraduate Research Symposium May 2021

References

- **Prof. Lisa Thompson**
  Professor, Department of Computer Sciences
  University of Wisconsin-Madison
  Email: lisa.thompson@wisc.edu
- **Prof. Maria Rodriguez**
  Professor, CSAIL
  Massachusetts Institute of Technology
  Email: maria.rodriguez@mit.edu