

Yang Gao

E-mail: gaoyang@iu.edu, Phone: 347-573-7642

Website: <https://dsail.kelley.iu.edu/members/phd/yang-gao.html>

Department of Operations and Decision Technologies
Indiana University Bloomington

Kelley School of Business
1275 E. 10th St, Bloomington, IN 47405

EDUCATION

Ph.D. , Information Systems, Indiana University, Bloomington	2022-2027 (Expected)
<ul style="list-style-type: none">• Minor: Data Science• Advisor: Dr. Sagar Samtani• Research Associate in Kelley's Data Science and Artificial Intelligence Lab	
M.S. , Business Analytics, Fordham University	2017-2019
<ul style="list-style-type: none">• Research Associate for Dr. Yilu Zhou	
B.Mgt. , Management Science, Fudan University	2013-2017

RESEARCH INTERESTS

1. **Applications:** Cybersecurity, Phishing Websites Detectors Evasion and Robustness
2. **Methods:** Deep Reinforcement Learning, Adversarial Learning, Large Language Models

JOURNAL PUBLICATIONS

1. A. Yuan, **Y. Gao**, E. Garcia, and S. Samtani, "Identifying Emotional Distress on Social Media: A Replication Study" *Forthcoming at AIS Transactions on Replication Research*.
2. **Y. Gao**, B. Ampel, and S. Samtani, "Evading Anti-Phishing Models: A Field Note Documenting an Experience in the Machine Learning Security Evasion Competition 2022" *ACM Digital Threats: Research and Practice (DTRAP)*, Volume 5, Issue 1, Pages 1-8, 2024.

JOURNAL PAPERS UNDER REVIEW

1. E. Garcia, **Y. Gao**, C. Sherwood-Laughlin, H. Zhu, A. Chow, S. Samtani, N. Liu, and J. Macy, "Exploring Mental Health Literacy Among IT Professionals: Twitter Content Analysis" *Invited for Second Round Review at PLOS Digital Health*.

WORK-IN-PROGRESS JOURNAL PAPERS

1. **Y. Gao**, B. Ampel, D. Zhou, and S. Samtani "Automated Adversarial Emulation to Examine the Robustness of Machine Learning-Based Phishing Website Detectors: A Reinforcement Learning Approach," *Targeted at Management Information Systems Quarterly (MISQ)*.
2. **Y. Gao**, B. Ampel, and S. Samtani, "Improving the Adversarial Robustness of Machine Learning-based Phishing Website Detectors: An Auxiliary Model with Attacker's Knowledge," *Targeted at Management Information Systems Quarterly (MISQ)*.

CONFERENCE PROCEEDINGS

1. **Y. Gao**, B. Ampel, and S. Samtani, "Examining the Robustness of Machine Learning-based Phishing Website Detection: Action-Masked Reinforcement Learning for Automated Red Teaming", IEEE Security and Privacy (IEEE S&P) Human-Machine Intelligence for Security Analytics (HMISA). San Francisco, CA, May 12-15, 2025.
2. A. Kathikar, B. Lazarine, **Y. Gao**, A. Shah, and S. Samtani, "Generating Secure Artificial Intelligence Model Source Code: A Reinforcement Learning Approach", IEEE Security and Privacy (IEEE S&P) Human-Machine Intelligence for Security Analytics (HMISA). San Francisco, CA, May 12-15, 2025.
3. **Y. Gao**, S. Samtani, and A. Shah, "Improving the Adversarial Robustness of Machine Learning-based Phishing Website Detectors: An Autoencoder-based Auxiliary Approach", Hawaii International Conference on Systems Sciences (HICSS). Waikoloa Village, Big Island, Hawaii, January 7-10, 2025.

- B. Ampel, **Y. Gao**, J. Hu, S. Samtani, and H. Chen, "Benchmarking the Robustness of Phishing Email Detection Systems" Americas Conference on Information Systems (AMCIS). Panama City, Panama. August 10-12, 2023.

REFEREED WORKSHOP PAPERS (No Proceedings)

- Y. Gao**, S. Samtani, H. Zhu, B. Ampel, and Y. Chai "Generating Adversarial Phishing Websites to Evade Machine Learning-based Anti-Phishing Detectors: A Reinforcement Learning Approach" In INFORMS 7th Workshop on Data Science, Phoenix, Arizona, October 2023.
- Y. Zhou, H. Sun, and **Y. Gao**, "Protecting Children from Inappropriate Mobile Apps: A Text and Image Deep Learning Approach" In INFORMS 2nd Workshop on Data Science, Phoenix, Arizona, October 2018.

INVITED TALKS

- Event Title:** Spring 2024 Institute for Digital Enterprise (IDE) Digital Unleashed: Bridging Research and Practice on AI, Cybersecurity, and Digital Transformation. **Talk Title:** Automated Adversary Emulation to Examine the Robustness of Machine Learning-based Phishing Website Detectors: A Reinforcement Learning Approach. Indiana University. April 19, 2024.

GRANT EXPERIENCE

- Year:** 2024. **Grant Title:** "SaTC: CORE: Medium: Automatic Phishing Generation and Detection Across Multiple Modalities: A Generative Artificial Intelligence and Reinforcement Learning Perspective" Funding Source: National Science Foundation. **Funding Request:** \$1.2M. **Status:** Declined. **Role:** Assisting Grant Writer.

TEACHING EXPERIENCE

Role	Course	Level	Method	# of Sections	# of Students	Institution	Semester
GTA	S364 Business Data Programming	Undergraduate	In-Person	3	134	Indiana U.	Fall 2023
GTA	Web Analytics	Master	In-Person	3	105	Fordham U.	Fall 2018
GTA	Machine Learning and Text Mining	PhD	In-Person	1	6	Fordham U.	Spring 2019

PROFESSIONAL SERVICE

Ad-hoc Reviewer (7 Conferences):

- The 30th European Symposium on Research in Computer Security (ESORICS), 2025.
- The AAAI-25 Workshop on Artificial Intelligence for Cyber Security (AICS), 2025.
- The Conference on Applied Machine Learning in Information Security (CAMLIS), 2024.
- The 34th Workshop on Information Technologies and Systems (WITS), 2024.
- The Pacific Asia Conference on Information Systems (PACIS), 2024.
- The 4th Workshop on Artificial Intelligence-Enabled Cybersecurity Analytics (AI4Cyber), 2024.
- The 7th INFORMS Workshop on Data Science (WDS), 2023.

Other Service to the Field (IS):

- Website Editor, Journal of Management Information Systems (JMIS), September 2023-Present.
- Website Editor, Kelley's Data Science and Artificial Intelligence Lab (DSAIL), September 2023-Present.
- Website Editor and Volunteer, Conference on Applied Machine Learning in Information Security (CAMLIS), 2023-2024.
- Website Editor, ACM KDD Workshop on AI-enabled Cybersecurity Analytics (AI4Cyber), 2023-2024.
- Program Committee Member, ACM KDD Workshop on AI-enabled Cybersecurity Analytics (AI4Cyber), 2024.
- Volunteer, Conference on Information Systems and Technology (CIST), 2022.
- Volunteer, The 6th INFORMS Workshop on Data Science (WDS), 2022.

AWARDS

- Institute for Digital Enterprise (IDE) Digital Unleashed The 2nd Place Presentation Award, Amount: \$1.75k. 2024.
- Data Science Workshop Best Reviewer Award, The INFORMS 7th Workshop on Data Science, Phoenix, Arizona, 2023.

PROFESSIONAL AFFILIATIONS AND SOCIETIES

1. Association for Information Systems (AIS), Member
2. Association for Computing Machinery (ACM), Member
3. Institute of Electrical and Electronics Engineers (IEEE), Member
4. Institute for Operations Research and the Management Sciences (INFORMS), Member

RELEVANT TECHNOLOGY SKILLS

1. **Databases:** MySQL, PostgreSQL, Neo4j AuraDB
2. **Programming Languages:** Python, C, PHP, SQL, Cypher
3. **Visualization tools:** Tableau, Gephi, Neo4j
4. **Data mining tools:** SPSS Modeler, Stata, WEKA, scikit-learn
5. **Major deep learning toolkits:** PyTorch, Keras, Tensorflow, Gymnasium, Ray RLlib
6. **Web development:** Heroku, Squarespace, GoDaddy

WORK EXPERIENCE

Ehomie New York Inc.	Texas Associate Manager & Business Analyst	February 2019 – February 2022
----------------------	--	----------------------------------

PROFESSIONAL REFERENCES

1. **Sagar Samtani, Ph.D.**
Associate Professor and Arthur M. Weimer Faculty Fellow
Executive Founding Director, Data Science and Artificial Intelligence Lab
Founding Editor-in-Chief, *ACM Transactions on AI Security and Privacy*
Kelley School of Business
Indiana University, Bloomington
Email: ssamtani@iu.edu
Phone: 812.855.8925
2. **Ramesh Venkataraman, Ph.D.**
John R. Gibbs Professor of Information Systems
Acting Co-Director, Data Science and Artificial Intelligence Lab
Dean, Hutton Honors College
Kelley School of Business Indiana University, Bloomington
Email: venkat@iu.edu
Phone: 812.855.2641
3. **Yilu Zhou, Ph.D.**
Associate Professor and Area Chair
Program Director, MS in Artificial Intelligence in Business
Gabelli School of Business
Fordham University
Email: yzhou62@fordham.edu
Phone: 202.494.8061