

Anindya Maiti

Devon Energy Hall 460, 110 W Boyd St, Norman, Oklahoma 73019, USA

am@ou.edu · +1 (316) 243-6204

[Personal Webpage](#) · [Lab Webpage](#) · [Lab GitHub](#) · [Google Scholar](#) · [LinkedIn](#) · [Instagram](#)

SCIENTIFIC INTERESTS

- Network and Internet Security
- Censorship Circumvention
- Decentralized Systems Security
- Human-Centered Privacy
- AI Security and Literacy
- Urban Micromobility Sensing

I develop secure, privacy-preserving, and trustworthy AI, software, and networked systems through rigorous, measurement-driven, human-centered cybersecurity research, with complementary work on urban micromobility sensing and safety. My research combines large-scale measurement, system design, and human-subject studies to identify emerging risks, characterize attacker and user behavior, and build practical defenses and sensing infrastructure across mobile, wearable, web, decentralized, and micromobility platforms.

EDUCATION

Doctor of Philosophy in Electrical Engineering and Computer Science May 2018

Wichita State University, Wichita, USA

Dissertation: *Security and Privacy of Cyber and Physical User Interactions in the Age of Wearable Computing*

Advisor: [Murtuza Jadliwala](#)

Master of Science in Electrical Engineering July 2014

Wichita State University, Wichita, USA

Thesis: *Context-Aware Access Control: An Alternate Privacy Protection Mechanism for Online Social Networks*

🏆 Outstanding Master's Thesis Award

Advisor: [Murtuza Jadliwala](#)

Bachelor of Technology in Computer Science and Engineering May 2012

Vellore Institute of Technology, Vellore, India

ACADEMIC APPOINTMENTS

Assistant Professor August 2020 – Present

University of Oklahoma, Norman, USA

School of Computer Science; Data Science and Analytics Institute

🏆 Outstanding Faculty Award, 2023

Postdoctoral Fellow July 2018 – August 2020

University of Texas at San Antonio, San Antonio, USA

Institute for Cyber Security; [SPriTELab](#)

Research Fellow February 2018 – May 2018

University of Texas at San Antonio, San Antonio, USA

Department of Computer Science

Graduate Research Assistant August 2013 – December 2017

Wichita State University, Wichita, USA

Department of Electrical Engineering and Computer Science

Summer Intern June 2011 – July 2011

Indian Institute of Technology Kharagpur, Kharagpur, India

Integrated Circuits and Systems Engineering Lab

PUBLICATIONS

3 research artifacts with 1,446 combined dataset downloads and 34 GitHub stars, 8 journal articles, 24 conference papers (including 1 USENIX Security Distinguished Paper), 8 workshop papers, 1 poster/demo, 3 reports/pre-prints, and 1 patent

application, with 1,150+ total citations; 4 manuscripts currently under review. Collaborated with 50+ co-authors across all works.

Datasets

3. Scott Seidenberger, Oluwasijibomi Ajisegiri, Noah Pursell, Fazil Raja, Anindya Maiti, “Why You’ve Got Mail: Evaluating Inbox Privacy Implications of Email Marketing Practices in Online Apps and Services”, *Academic Torrents*, 2025. 📄 1,143 downloads.
2. Joseph Spracklen, Raveen Wijewickrama, AHM Sakib, Anindya Maiti, Bimal Viswanath, Murtuza Jadliwala, “We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs”, *GitHub*, 2025. ★ 34 stars.
1. Scott Seidenberger, Noah Pursell, Anindya Maiti, “MagnetDB: A Longitudinal Torrent Discovery Dataset with IMDb-Matched Movies and TV Shows”, *Academic Torrents*, 2025. 📄 303 downloads.

Peer-Reviewed Journal Articles

8. Scott Seidenberger, Noah Pursell, Anindya Maiti, “Front-Running the Red Carpet: A Measurement Study of Media Torrent Leaks and User Risks”, *Journal of Quantitative Description: Digital Media (JQD:DM)*, 2026.
7. Raveen Wijewickrama, Sameer Anis Dohadwalla, Anindya Maiti, Murtuza Jadliwala, Sashank Narain, “SkinSense: Efficient Vibration-Based Communications over Human Body Using Motion Sensors”, *Elsevier Internet of Things (IoT)*, 2023.
6. Anindya Maiti, Murtuza Jadliwala, “Smart Light-Based Information Leakage Attacks”, *ACM GetMobile: Mobile Computing and Communications*, 2020.
5. Anindya Maiti, Murtuza Jadliwala, “Light Ears: Information Leakage via Smart Lights”, *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)*, 2019. Presented at **UbiComp 2019**. 📄 60+ citations.
4. Anindya Maiti, Murtuza Jadliwala, Jibo He, Igor Bilogrevic, “Side-Channel Inference Attacks on Mobile Keypads Using Smartwatches”, *IEEE Transactions on Mobile Computing (TMC)*, 2018. 📄 60+ citations.
3. Mohammad Hossein Manshaei, Murtuza Jadliwala, Anindya Maiti, Mahdi Fooladgar, “A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains”, *IEEE Access*, 2018. 📄 80+ citations.
2. Nisha Vinayaga-Sureshkanth, Anindya Maiti, Murtuza Jadliwala, Kirsten Crager, Jibo He, Heena Rathore, “A Practical Framework for Preventing Distracted Pedestrian-Related Incidents Using Wrist Wearables”, *IEEE Access*, 2018.
1. Arash Boustani, Anindya Maiti, Sina Yousefian Jazi, Murtuza Jadliwala, Vinod Nambodiri, “Seer Grid: Privacy and Utility Implications of Two-Level Load Prediction in Smart Grids”, *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 2017.

Peer-Reviewed Conference Papers

24. Taylor Wise, Scott Seidenberger, Anindya Maiti, “What Should I Become? When LLMs Present a Slice of Opportunity as the Whole”, *AAAI/ACM Conference on AI, Ethics, and Society (AIES)*, Malmö, Sweden, October 2026.
23. Raveen Wijewickrama, Maryam Abbasi-hafshejani, Anindya Maiti, Murtuza Jadliwala, “OverHear: Headphone Based Multi-Sensor Keystroke Inference”, *International Conference on Applied Cryptography and Network Security (ACNS)*, Stony Brook, New York, USA, June 2026.
22. Khoi Trinh, Scott Seidenberger, Joseph Spracklen, Raveen Wijewickrama, Bimal Viswanath, Murtuza Jadliwala, Anindya Maiti, “Prompt and Circumstances: Evaluating the Efficacy of Human Prompt Inference in AI-Generated Art”, *International Conference on Artificial Intelligence in Music, Sound, Art and Design (EvoMUSART)*, Toulouse, France, April 2026.
21. Scott Seidenberger, Anindya Maiti, “From Big Data to Valued Data: A Dataset Value Taxonomy for AI-Native Empirical Research”, *AAAI/ACM Conference on AI, Ethics, and Society (AIES)*, Madrid, Spain, October 2025.
20. Scott Seidenberger, Anindya Maiti, “Initial Evidence of Pervasive Reconnaissance Targeting Ethereum Node Infrastructure”, *ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI)*, Hanoi, Vietnam, August 2025.

19. Khoi Trinh, Scott Seidenberger, Raveen Wijewickrama, Murtuza Jadliwala, Anindya Maiti, “A Picture Is Worth a Thousand Prompts? Efficacy of Iterative Human-Driven Prompt Refinement in Image Regeneration Tasks”, *International Joint Conference on Artificial Intelligence (IJCAI)*, Montreal, Canada, August 2025.
18. Joseph Spracklen, Raveen Wijewickrama, AHM Sakib, Anindya Maiti, Bimal Viswanath, Murtuza Jadliwala, “We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs”, *USENIX Security Symposium*, Seattle, Washington, USA, August 2025. 🏆 Distinguished Paper Award. 📄 170+ citations.
17. Scott Seidenberger, Noah Pursell, Anindya Maiti, “MagnetDB: A Longitudinal Torrent Discovery Dataset with IMDb-Matched Movies and TV Shows”, *International AAAI Conference on Web and Social Media (ICWSM)*, Copenhagen, Denmark, June 2025.
16. Scott Seidenberger, Oluwasijibomi Ajisegiri, Noah Pursell, Fazil Raja, Anindya Maiti, “Why You’ve Got Mail: Evaluating Inbox Privacy Implications of Email Marketing Practices in Online Apps and Services”, *ACM Conference on Data and Application Security and Privacy (CODASPY)*, Pittsburgh, Pennsylvania, USA, June 2025.
15. Scott Seidenberger, Anindya Maiti, “EtherBee: A Global Dataset of Ethereum Node Performance Measurements Coupled with Honeypot Interactions and Full Network Sessions”, *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Pisa, Italy, June 2025.
14. Maryam Abbasihafshejani, Anindya Maiti, Murtuza Jadliwala, “Spiking Neural Networks in Vertical Federated Learning: Performance Trade-Offs”, *IEEE/IFIP Network Operations and Management Symposium (NOMS)*, Honolulu, Hawaii, USA, May 2025.
13. Kavita Kumari, Murtuza Jadliwala, Sumit Kumar Jha, Anindya Maiti, “Towards a Game-Theoretic Understanding of Explanation-Based Membership Inference Attacks”, *Conference on Decision and Game Theory for Security (GameSec)*, New York City, New York, USA, October 2024.
12. Mohd Sabra, Nisha Vinayaga-Sureshkanth, Ari Sharma, Anindya Maiti, Murtuza Jadliwala, “De-Anonymizing VR Avatars Using Non-VR Motion Side-Channels”, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Seoul, Korea, June 2024.
11. Mohd Sabra, Anindya Maiti, Murtuza Jadliwala, “Background Buster: Peeking Through Virtual Backgrounds in Online Video Calls”, *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Baltimore, Maryland, USA, June 2022.
10. Nisha Vinayaga-Sureshkanth, Raveen Wijewickrama, Anindya Maiti, Murtuza Jadliwala, “An Investigative Study on the Privacy Implications of Mobile E-Scooter Rental Apps”, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, San Antonio, Texas, USA, May 2022.
9. Soundarya Ramesh, Rui Xiao, Anindya Maiti, Jong Taek Lee, Harini Ramprasad, Ananda Kumar, Murtuza Jadliwala, Jun Han, “Acoustics to the Rescue: Physical Key Inference Attack Revisited”, *USENIX Security Symposium*, Virtual, August 2021.
8. Raveen Wijewickrama, Anindya Maiti, Murtuza Jadliwala, “Write to Know: On the Feasibility of Wrist Motion Based User-Authentication from Handwriting”, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Virtual, June 2021.
7. Mohd Sabra, Anindya Maiti, Murtuza Jadliwala, “Zoom on the Keystrokes: Exploiting Video Calls for Keystroke Inference Attacks”, *Network and Distributed System Security Symposium (NDSS)*, Virtual, February 2021.
6. Kavita Kumari, Murtuza Jadliwala, Anindya Maiti, Mohammad Hossein Manshaei, “Analyzing Defense Strategies Against Mobile Information Leakages: A Game-Theoretic Approach”, *Conference on Decision and Game Theory for Security (GameSec)*, Stockholm, Sweden, October 2019.
5. Raveen Wijewickrama, Anindya Maiti, Murtuza Jadliwala, “deWristified: Handwriting Inference Using Wrist-Based Motion Sensors Revisited”, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Miami, Florida, USA, May 2019.
4. Anindya Maiti, Ryan Heard, Mohd Sabra, Murtuza Jadliwala, “Towards Inferring Mechanical Lock Combinations Using Wrist-Wearables as a Side-Channel”, *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Stockholm, Sweden, June 2018.
3. Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, Jibo He, “Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms”, *ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, Xi’an, China, May 2016. 📄 120+ citations.

2. Anindya Maiti, Murtuza Jadliwala, Jibo He, Igor Bilogrevic, “(Smart)Watch Your Taps: Side-Channel Keystroke Inference Attacks Using Smartwatches”, *ACM International Symposium on Wearable Computers (ISWC)*, Osaka, Japan, September 2015. 📄 60+ citations.
1. Murtuza Jadliwala, Anindya Maiti, Vinod Namboodiri, “Social Puzzles: Context-Based Access Control in Online Social Networks”, *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Atlanta, Georgia, USA, June 2014.

Peer-Reviewed Workshop Papers

8. Scott Seidenberger, Marc Beret, Raveen Wijewickrama, Murtuza Jadliwala, Anindya Maiti, “NinjaDoH: A Censorship-Resistant Moving Target DoH Server Using Hyperscalers and IPNS”, *Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb, co-located with NDSS)*, San Diego, California, USA, February 2026.
7. Anindya Maiti, Nisha Vinayaga-Sureshkanth, Murtuza Jadliwala, Raveen Wijewickrama, Greg P. Griffin, “Impact of E-Scooters on Pedestrian Safety: A Field Study Using Pedestrian Crowd-Sensing”, *IEEE PerCom Workshop on Sensing Systems and Applications using Wrist Worn Smart Devices (WristSense)*, Pisa, Italy, March 2022. 📄 70+ citations.
6. Nisha Vinayaga-Sureshkanth, Raveen Wijewickrama, Anindya Maiti, Murtuza Jadliwala, “Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems”, *ACM Workshop on Automotive and Aerial Vehicle Security (AutoSec)*, Virtual, August 2020.
5. Mohd Sabra, Anindya Maiti, Murtuza Jadliwala, “Keystroke Inference Using Ambient Light Sensor on Wrist-Wearables: A Feasibility Study”, *ACM MobiSys Workshop on Wearable Systems and Applications (WearSys)*, Munich, Germany, June 2018.
4. Nisha Vinayaga-Sureshkanth, Anindya Maiti, Murtuza Jadliwala, Kirsten Crager, Jibo He, Heena Rathore, “Towards a Practical Pedestrian Distraction Detection Framework Using Wearables”, *IEEE PerCom Workshop on Sensing Systems and Applications using Wrist Worn Smart Devices (WristSense)*, Athens, Greece, March 2018. 🏆 Apple Best Paper Award.
3. Anindya Maiti, Kirsten Crager, Murtuza Jadliwala, Jibo He, Kevin Kwiat, Charles Kamhoua, “RandomPad: Usability of Randomized Mobile Keypads for Defeating Inference Attacks”, *IEEE EuroS&P Workshop on Innovations in Mobile Privacy & Security (IMPS)*, Paris, France, April 2017.
2. Kirsten Crager, Anindya Maiti, Murtuza Jadliwala, Jibo He, “Information Leakage Through Mobile Motion Sensors: User Awareness and Concerns”, *European Workshop on Usable Security (EuroUSEC)*, Paris, France, April 2017.
1. Anindya Maiti, Murtuza Jadliwala, Chase Weber, “Preventing Shoulder Surfing Using Randomized Augmented Reality Keyboards”, *IEEE PerCom Workshop on Security, Privacy and Trust in the Internet of Things (SPT-IoT)*, Kona, Hawaii, USA, March 2017. 📄 50+ citations.

Peer-Reviewed Posters and Demos

1. Ubaidullah Khan, Raveen Wijewickrama, Buddhi Ashan M.K., AHM Sakib, Khoi Trinh, Christina Duthie, Nima Najafian, Ahmer Patel, R.N. Molina, Anindya Maiti, Sushil K. Prasad, Greg P. Griffin, Murtuza Jadliwala, “ScooterLab: A Programmable and Participatory Sensing Research Testbed Using Micromobility Vehicles”, *IEEE International Conference on Pervasive Computing and Communications (PerCom) Demos*, Washington, D.C., USA, March 2025.

Reports and Pre-Prints

3. Khoi Trinh, Joseph Spracklen, Raveen Wijewickrama, Bimal Viswanath, Murtuza Jadliwala, Anindya Maiti, “Promptly Yours? A Human Subject Study on Prompt Inference in AI-Generated Art”, [arXiv:2410.08406](https://arxiv.org/abs/2410.08406), 2024.
2. Noah Pursell, Anindya Maiti, “Generating Print-Ready Personalized AI Art Products from Minimal User Inputs”, [arXiv:2405.18247](https://arxiv.org/abs/2405.18247), 2024.
1. Scott Seidenberger, Alec Sokol, Anindya Maiti, “Stake Your Claim: Zero-Trust Validator Deployment Leveraging NFTs and Smart Contracts in Proof-of-Stake Networks”, [arXiv:2308.01158](https://arxiv.org/abs/2308.01158), 2023.

Patent Applications

1. Murtuza Jadliwala, Anindya Maiti, “Blockchain Game”, US Patent Application 16/856,782, filed April 2020.

Under Review

4. Anindya Maiti, “Block-A-Mole: The Sustainability Frontier of Moving-Target Censorship Resistance”, under review at *IEEE Symposium on Security and Privacy (S&P/Oakland)*, 2027.
3. Scott Seidenberger, Khoi Trinh, Anindya Maiti, “Node Infrastructure First: Measuring Attacks, Modeling Cascades, and Rapid Recovery Tactics for Public Blockchains”, under review at *ACM Distributed Ledger Technologies (DLT)*, 2026.
2. Khoi Trinh, Jay Rothenberger, Scott Seidenberger, Dimitrios I. Diochnos, Anindya Maiti, “CLPIPS: A Personalized Metric for AI-Generated Image Similarity”, under review at *Transactions on Machine Learning Research (TMLR)*, 2026.
1. Khoi Trinh, Scott Seidenberger, Raveen Wijewickrama, Murtuza Jadliwala, Anindya Maiti, “The Refinement Gap: A Mixed-Effects Comparison of Human and Agentic Prompt Refinement in Image Regeneration”, under review at *Transactions on Machine Learning Research (TMLR)*, 2026.

GRANTS

\$354,918 attributed to him across 5 awards as PI or Co-PI, from the National Science Foundation, the Ethereum Foundation, and the University of Oklahoma’s Data Institute for Societal Challenges, within collaborative projects totalling \$2,068,080; \$2.7M+ in NSF proposals currently under review.

External Grants

Funded

4. *Change Analysis and Network Anomaly Recognition sYstem (CANARY)*
Funding Agency: Ethereum Foundation (Academic Grant FY24-1546)
Investigators: Anindya Maiti, Scott Seidenberger
Role: Principal Investigator (PI)
Total Award Amount: \$23,985.48
Attributed Effort: 50%
July 2024 – May 2026
3. *Secure Ethereum Anonymity & Defense Relay via Advanced Global Overlay Networking (SEADRAGON)*
Funding Agency: Ethereum Foundation (Academic Grant FY24-1547)
Investigators: Anindya Maiti, Scott Seidenberger
Role: Principal Investigator (PI)
Total Award Amount: \$17,368.00
Attributed Effort: 50%
July 2024 – May 2026
2. *NSF Collaborative Research: CCRI: New: ScooterLab – A Programmable and Participatory Sensing Testbed using Micromobility Vehicles*
Funding Agency: National Science Foundation (Award Numbers 2234516 and 2234517)
Investigators: Murtuza Jadliwala, Sushil Prasad, Greg Griffin, Anindya Maiti
OU Role: Principal Investigator (PI)
Total Award Amount: \$1,919,062 (OU: \$205,900)
OU Attributed Effort: 100%
March 1, 2023 – February 28, 2027
1. *NSF CCRI: Planning: ScooterLab: Development of a Programmable and Participatory e-Scooter Testbed to Enable CISE-focused Micromobility Research*
Funding Agency: National Science Foundation (Award Number 2016717)
Investigators: Murtuza Jadliwala, Anindya Maiti, Sushil Prasad, Greg Griffin
Role: Co-Principal Investigator (Co-PI)
Total Award Amount: \$100,000
Attributed Effort: 25%
October 1, 2020 – March 31, 2023

Under Review

4. *CAREER: Theoretical Foundations of Moving-Target Censorship Resistance: Timing Games, Information-Theoretic Limits, and Adaptive Defense on Hyperscaler Clouds*
Funding Agency: National Science Foundation
Investigators: Anindya Maiti
Role: Principal Investigator (PI)
Total Anticipated Amount: \$665,276
Attributed Effort: 100%
5-Year Project Duration
3. *SoonerAI: A Gamified Agent-Building Platform for Multi-Disciplinary Data Science Learning in K-12 Education*
Funding Agency: National Science Foundation
Investigators: Anindya Maiti, Doga Demirel, Dimitrios Diochnos, Danny Mattox
Role: Principal Investigator (PI)
Total Anticipated Amount: \$749,852
Attributed Effort: 25%
3-Year Project Duration

2. *C4-Math: AI-Mediated Collaborative Mathematical Reasoning in Middle-School Classrooms*

Funding Agency: National Science Foundation

Investigators: Doga Demirel, Anindya Maiti, Danny Mattox

Role: Co-Principal Investigator (Co-PI)

Total Anticipated Amount: \$749,999

Attributed Effort: 33%

3-Year Project Duration

1. *Cross-Cutting Improvements: TRACE – Trustworthy Reproducibility through Agent-assisted Computational Evaluation*

Funding Agency: National Science Foundation

Investigators: Anindya Maiti

Role: Principal Investigator (PI)

Total Anticipated Amount: \$599,977

Attributed Effort: 100%

3-Year Project Duration

Internal Grants

Funded

1. *Enhancing Email Management through Large Multi-Modal Model Classification*

Funding Agency: Data Institute for Societal Challenges (DISC), University of Oklahoma

Investigators: Anindya Maiti

Role: Principal Investigator (PI)

Total Award Amount: \$7,665

Attributed Effort: 100%

May 2025 – December 2025

TEACHING

4 lecture courses taught (2 developed as founding instructor) at the University of Oklahoma since 2020, reaching 691+ students across undergraduate and graduate programs.

Courses

Lecture Courses at University of Oklahoma (as Faculty):

- **CS 5193 – Cyber Attacks & Defenses (Founding Instructor)**
Term and Year Taught (Enrollment): Spring 2024 (40), Spring 2025 (38), Spring 2026 (11)
- **CS 5833 – Blockchains & Cryptocurrencies (Founding Instructor)**
Term and Year Taught (Enrollment): Spring 2022 (30), Spring 2023 (30+1), Spring 2024 (40), Spring 2025 (39), Spring 2026 (15)
- **CS 5903 – Perspectives on Computing**
Term and Year Taught (Enrollment): Fall 2025 (21, co-instructed with Dr. Song Fang)
- **CS 2334 – Programming Structures and Abstractions**
Term and Year Taught (Enrollment): Fall 2020 (50), Fall 2021 (56), Fall 2022 (51+56), Spring 2023 (213)

Research-Oriented Courses at University of Oklahoma (as Faculty):

- **CS 5990 / DSA 5990 – Independent Study**
Mentored 16 graduate students: Olivia Black, Sai Prakash Davuluri, Catherine Donner, Mahmoud Mousa Hamad, Natalie Hill, Kristiana Karshelieva, Taylor Keller, Sai Siddhardha Maguluri, Narayana Phani Charan Nimmagadda, Fazil Raja, Brandon Robertiello, Scott Seidenberger, Clark Smith, Khoi Trinh, Koy Wilson, Chris Womack.
- **CS 3440 – Mentored Research Experience**
Mentored 8 undergraduate students: Daylon Carse, Preston Jones, Kristiana Karshelieva, Aleo Lo, Nima Najafian, Noah Pursell, Koy Wilson, Taylor Wise.
- **CS 3450 – Undergraduate Research**
Mentored 2 undergraduate students: Roman Beames, Nathan Sandoval.
- **CS 3980 – Honors Research**
Mentored 3 undergraduate students: Luke Kirk, Haidyn Peterson, Taylor Wise.

ADVISING

Primary advisor for 2 current and 1 graduated PhD students (plus 1 reassigned), and 2 current and 2 graduated Master's thesis students; mentored 4 current and 22 past graduate students in total, alongside 1 current and 10 past undergraduate research students (16 OU undergraduates in total, 8 of whom continued into the BS+MS program and are listed above under graduate students); additionally served on 15 thesis/dissertation committees as a member (not primary advisor).

Supervision of Graduate Research Students

Current Graduate Students:

- 👤 Oluwasijibomi Ajisegiri – PhD in Computer Science.
 - Dissertation Topic: *Email Inbox Privacy and Novel AI-Assisted Email Classification Methods*.
- 👤 Khoi Trinh – PhD in Data Science and Analytics.
 - Dissertation Topic: *Human-AI and Human-vs.-AI Interactions in Image Regeneration Tasks*.
 - Other Works: *Development of the ScooterLab Fleet Controller System* (with Nima Najafian, Kristiana Karshelieva, Taylor Keller).
- 👤 Noah Pursell – BS in Computer Science (2026) + MS in Computer Science (Thesis).
 - Thesis Topic: *Developing Defense Mechanisms Against Prompt Injection Attacks on Large Language Models*.
 - Other Works: *Performance Analysis of Text-to-Image Generation and Image Upscaling Models; Analysis of Inbox Privacy Implications of Email Marketing Practices in Online Apps and Services* (with Scott Seidenberger, Oluwasijibomi Ajisegiri, Fazil Raja); *Measurement of Media Torrent Discovery and Associated User Privacy Risks* (with Scott Seidenberger).
 - 🏆 Honors College Undergraduate Research Opportunities Program (UROP) Award (2024).
 - 🏆 GCoE Research Fellowship (2023).
 - 🏆 GCoE Research Entry Apprenticeship (2023).
- 👤 Taylor Wise – BS in Computer Science (2026) + MS in Computer Science (Thesis).
 - Thesis Topic: *Investigating Representational Bias in LLM-Generated Career Recommendations*.
 - Other Works: *Benchmarking GPU Utilization Across LLMs and Workloads for Distributed GPU Cluster Trade-off and Cost Estimation* (with Haidyn Peterson).

Past Graduate Students:

At University of Oklahoma (as Primary Faculty Advisor):

- 👤 Scott Seidenberger – PhD in Data Science and Analytics (Graduated 2026).
 - Dissertation: *Toward a General Science of Secure Protocol Networks: Measuring and Improving Privacy, Security, and Resilience in Planet-Scale Decentralized Systems*.
 - 🏆 GCoE Dissertation Excellence Award (2026).
- 👤 Marc Beret – MS in Computer Science (Thesis, Graduated 2024).
 - Thesis: *Evaluation of Moving Target DoH Server Detection Using Machine Learning Models*.
- 👤 Tristan Bony – MS in Computer Science (Thesis, Graduated 2024).
 - Thesis: *Evaluating the Impact of External Factors on the Stability of the Ethereum Network*.
- 👤 Olivia Black – MS in Computer Science (Independent Study, Graduated 2022).
 - Topic: *A Review of Modern Deep Learning Algorithms and Architectures in Applications of Natural Language Processing*.
- 👤 Sai Prakash Davuluri – MS in Computer Science (Independent Study, Graduated 2023).
 - Topic: *A Comparative Quality-of-Service Analysis Between Centralized and Decentralized Cloud Storage*.
- 👤 Mahmoud Mousa Hamad – MS in Computer Science (Independent Study, Graduated 2022).
 - Topic: *JobApplier: Towards Automation of Online Job Applications*.
- 👤 Natalie Hill – MS in Computer Science (Independent Study, Graduated 2025).
 - Topic: *AI Politician: Fine-tuned Models for Political Discourse* (with Preston Jones).
- 👤 Kristiana Karshelieva – BS in Computer Science (2025) + MS in Computer Science (Independent Study, Graduated 2026).
 - Topic: *Zero-Shot Classification Pipeline for 3D Printable Objects*.
 - Other Works: *Experiments with Generative Text Models for Long-Form Novels and with Generative Audio Models; Performance Optimization of the ScooterLab Fleet Controller System* (with Khoi Trinh).
 - 🏆 GCoE Research Fellowship (2024).
 - 🏆 Provost's Undergraduate Research and Creative Activity (URCA) Fellowship (2024).
 - 🏆 GCoE Research Entry Apprenticeship (2024).
- 👤 Taylor Keller – BS in Computer Science (2024) + MS in Data Science and Analytics (Independent Study, Graduated 2025).
 - Topic: *Optimization of ScooterLab Fleet Controller Databases and APIs* (with Khoi Trinh).

- 👤 Sai Siddhardha Maguluri – MS in Computer Science (Independent Study, Graduated 2023).
 - Topic: *Torrent Categorization and Evolutionary Analysis of Shared Content*.
- 👤 Narayana Phani Charan Nimmagadda – MS in Computer Science (Independent Study, Graduated 2025).
 - Topic: *From Pirated Media to High-Risk 3D Models: Mining MagnetDB-style Torrent Datasets for Societal Risk Insights*.
- 👤 Fazil Raja – BS in Computer Science (2023) + MS in Computer Science (Independent Study, Graduated 2023).
 - Topic: *Decoding Email Address Privacy: An In-depth Analysis of Data Management Practices in Popular Online Services* (with Scott Seidenberger, Oluwasijibomi Ajisegiri, Noah Pursell).
- 👤 Brandon Robertiello – BS in Computer Science (2025) + MS in Computer Science (Independent Study, Graduated 2025).
 - Topic: *General Purpose Hacker Registration Portal for Hacklahoma*.
- 👤 Clark Smith – BS in Computer Science (2025) + MS in Computer Science (Independent Study, Graduated 2025).
 - Topic: *A Language Model-Based Approach to Binary Similarity and Malicious Code Detection*.
- 👤 Koy Wilson – BS in Computer Science (2024) + MS in Computer Science (Independent Study, Graduated 2024).
 - Topic: *Machine Learning Approaches for Predictive Modeling of Sports Betting Outcomes* (with Daylon Carse).
- 👤 Chris Womack – MS in Computer Science (Independent Study, Graduated 2023).
 - Topic: *Towards Education 4.0, Powered By Modern AI Technologies*.

At University of Texas at San Antonio (Co-Mentored as Postdoctoral Fellow):

- 👤 Kavita Kumari – PhD in Computer Science (Graduated 2022).
 - Dissertation: *When and How to Protect? Modeling Repeated Interactions with Computing Services under Uncertainty*.
- 👤 Mohd Sabra – PhD in Computer Science (Graduated 2023).
 - Dissertation: *Addressing Privacy Challenges in Modern Audio-Video Communication Systems and Applications*.
- 👤 Nisha Vinayaga-Sureshkanth – PhD in Computer Science (Graduated 2025).
 - Dissertation: *Pedestrian Safety, Security and Privacy in the Era of Pervasive Mobile and Ubiquitous Computing*.
- 👤 Raveen Wijewickrama – PhD in Computer Science (Graduated 2024).
 - Dissertation: *Friend or Foe? Evaluating Sensor-Based Information Side-Channels and Covert Communication Channels on Modern Wearable Devices*.
- 👤 Comfort Olorunlero – MS in Computer Science (Thesis, Graduated 2021).
 - Thesis: *Evaluating the Privacy and Security Implications of Ambient Light Sensors on Modern Mobile Devices*.

At Wichita State University (Co-Mentored as Doctoral Student):

- 👤 Zoya Khan – MS in Computer Networking (Thesis, Graduated 2015).
 - Thesis: *An Evaluation of the Effectiveness of Smart Meter Data Perturbation Mechanisms Using a Unified Stochastic Framework*.

Reassigned Graduate Students (transitioned to other advisors):

- 👤 Catherine Donner – PhD in Data Science and Analytics, University of Oklahoma.
 - DoD SMART Scholarship.

Supervision of Undergraduate Research Students

Current Undergraduate Students:

- 👤 Nathan Sandoval – BS in Computer Science.
 - 🦋 GCoE Research Entry Apprenticeship (2026).

Past Undergraduate Students:

At University of Oklahoma (as Faculty):

- 👤 Roman Beames – BS in Computer Science (Graduated 2026).
 - Topic: *A Language Model-Based Approach to Binary Similarity and Malicious Code Detection* (extended initial work done by Clark Smith).
- 👤 Daylon Carse – BS in Computer Science (Graduated 2024).

- Topic: *Machine Learning Approaches for Predictive Modeling of Sports Betting Outcomes* (with Koy Wilson).

 Preston Jones – BS in Computer Science (Graduated 2025).

- Topic: *AI Politician: Fine-tuned Models for Political Discourse* (with Natalie Hill).

 Luke Kirk – BS in Computer Science (Graduated 2024).

- Topic: *Experimenting with the LangChain Framework for Agentic Applications*.

 Aleo Lo – BS in Computer Science (Graduated 2026).

- Topic: *Experimenting with the OpenClaw Framework for Agentic Applications*.

 Nima Najafian – BS in Computer Science (Graduated 2025).

- Topic: *ScooterLab Sensor Data Logging and Upload Framework Development* (with Khoi Trinh).

-  GCoE Research Fellowship (2023).

-  GCoE Research Entry Apprenticeship (2023).

 Haidyn Peterson – BS in Computer Science (Graduated 2026).

- Topic: *Benchmarking GPU Utilization Across LLMs and Workloads for Distributed GPU Cluster Trade-off and Cost Estimation* (with Taylor Wise).

At Wichita State University (Co-Mentored as Doctoral Student):

 Oscar Armbruster – BS in Computer Science (Graduated 2016).

 Ryan Heard – BS in Computer Science (Graduated 2017).

 Chase Weber – BS in Computer Engineering (Graduated 2017).

Thesis and Dissertation Committee Service (Not as Primary Advisor)

Doctoral Dissertation Committees:

 Pantia-Marina Alchirch – In Progress, University of Oklahoma (Advisor: Dr. Dimitrios Diochnos).

 Qiuye He – Graduated 2023, University of Oklahoma (Advisor: Dr. Song Fang).

 Yan He – Graduated 2026, University of Oklahoma (Advisor: Dr. Song Fang).

 Kavita Kumari – Graduated 2022, University of Texas at San Antonio (Advisor: Dr. Murtuza Jadliwala).

 Maisha Maliha – In Progress, University of Oklahoma (Advisor: Dr. Dean Hougen).

 Mohd Sabra – Graduated 2023, University of Texas at San Antonio (Advisor: Dr. Murtuza Jadliwala).

 Triet Tran – Graduated 2025, University of Oklahoma (Advisor: Dr. Sina Khanmohammadi).

 Nisha Vinayaga-Sureshkanth – Graduated 2025, University of Texas at San Antonio (Advisor: Dr. Murtuza Jadliwala).

 Raveen Wijewickrama – Graduated 2024, University of Texas at San Antonio (Advisor: Dr. Murtuza Jadliwala).

Master's Thesis Committees:

 Yan He – Graduated 2023, University of Oklahoma (Advisor: Dr. Song Fang).

 Moez Ullah Khan – Graduated 2026, University of Oklahoma (Advisor: Dr. Richard Veras).

 Tiffany Le – In Progress, University of Oklahoma (Advisor: Dr. Dimitrios Diochnos).

 Kyumin Lee – Graduated 2026, University of Oklahoma (Advisor: Dr. Song Fang).

 Mehdi Zaeifi – In Progress, University of Oklahoma (Advisor: Dr. Sina Khanmohammadi).

 Yan Zhou – Graduated 2024, University of Oklahoma (Advisor: Dr. Song Fang).

SERVICE & OUTREACH ACTIVITIES

Editor for 1 journal article; program committee for 3 conferences; reviewer for 8 journals and 4 conferences. 3 student organization advisor roles, 9 workshop/conference/summer-camp organizer roles, and 1 mentorship role.

Institutional Service

Department Service

- Committee Member, Graduate Studies Committee, OU School of Computer Science (2026 – Present).
- Committee Member, Graduate Program Assessment Committee, OU School of Computer Science (2026 – Present).

- Committee Member, Computing Committee, OU School of Computer Science (2025 – 2026).
- Committee Member, Tenure-Track Assistant Professor (Cybersecurity) Faculty Search Committee, OU School of Computer Science (2024 – 2025).
- Committee Member, Student Engagement Committee, OU School of Computer Science (2020 – 2023).

College Service

- Committee Member, GCoE Outstanding Senior Selection Committee (2022 – Present).
- Faculty Host for Prospective Computer Science Student Recruitment Visits, Visit Engineering (2020 – Present).
 - Hosted 34 prospective high school students exploring Computer Science studies at OU to date.

University Service

- Faculty Panelist, English Training and Certification Services, University of Oklahoma (2021 – Present).

Professional Service

Editorial Service

- Editor, *Frontiers in Psychology* (Cognitive Science section), 2026.

Conference Program Committees

- Program Committee Member, ACM Web Conference (WWW) 2026.
- Program Committee Member, IEEE Symposium on Security and Privacy (S&P) 2024.
- Program Committee Member, Network and Distributed System Security Symposium (NDSS) 2026.

Journal Reviewing

- ACM Distributed Ledger Technologies (DLT) (4 articles).
- ACM Transactions on Privacy and Security (TOPS) (1 article).
- ACM Transactions on Software Engineering and Methodology (TOSEM) (3 articles).
- Elsevier Pervasive and Mobile Computing (PMC) (2 articles).
- IEEE Transactions on Dependable and Secure Computing (TDSC) (1 article).
- IEEE Transactions on Mobile Computing (TMC) (1 article).
- IEEE/ACM Transactions on Networking (ToN) (1 article).
- Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/UbiComp) (2 articles).

Conference and Workshop Reviewing

- ACM Asia Conference on Computer and Communications Security (AsiaCCS) 2026 (3 papers).
- ACM Web Conference (WWW) 2026 (3 papers).
- International Joint Conference on Artificial Intelligence / European Conference on Artificial Intelligence (IJCAI-ECAI) 2026 (2 papers).
- Network and Distributed System Security Symposium (NDSS) 2026 (10 papers).

Community Engagement and Outreach

Leadership and Advisory Roles

- Community Outreach Director, [ScooterLab](#) (March 2023 – Present).
- Faculty Advisor, [Hacklahoma](#) (Student Organization), University of Oklahoma (2022 – Present).
- Faculty Advisor, Cybersecurity Club (Student Organization), University of Oklahoma (July 2024 – Present).
- Faculty Advisor, [Google Developers Group \(GDG\) on Campus at OU](#) (Student Organization), University of Oklahoma (October 2024 – Present).

Conference, Workshop, and Summer Camp Organization

- Co-Chair, [17th Central Area Networking and Security Workshop \(CANSec\)](#), University of Oklahoma, Norman, Oklahoma (2024).
- Publicity Chair, [15th ACM Conference on Security and Privacy in Wireless and Mobile Networks \(WiSec\)](#), San Antonio, Texas (2022).
- Workshop Co-Organizer, [ScooterLab Workshop 2026](#), San Antonio, Texas (May 2026).
- Workshop Co-Organizer, [ScooterLab Workshop 2025](#), San Antonio, Texas (May 2025).
- Workshop Co-Organizer, [ScooterLab Community Micromobility Research Workshop 2](#), Virtual (June 2021).
- Workshop Co-Organizer, [ScooterLab Community Micromobility Research Workshop 1](#), Virtual (November 2020).
- Summer Camp Co-Host, [Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques](#), San Antonio, Texas (June 2024).
- Summer Camp Co-Host, [Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques](#), San Antonio, Texas (June 2023).
- Summer Camp Co-Host, [Cyber Warriors: A Comprehensive Introduction to Cybersecurity Tools and Techniques](#), San Antonio, Texas (June 2022).

Mentorship for Underrepresented Communities in Computing

- Reboot Representation Mentor for Native American Women (2022 – 2025).
 - Mentee: [Madylin Teel](#), BS in Computer Science, University of Oklahoma.

Invited Talks, Demos, and Panels

- Invited Talk, [“Serverless on Google Cloud Workshop”](#), Google Developers Group (GDG) on Campus at OU, University of Oklahoma, Norman, Oklahoma (August 2026).
- Invited Talk, [“Hacklahoma Vibe Coding Workshop – Pokemon Edition”](#), Hacklahoma, University of Oklahoma, Norman, Oklahoma (November 2025).
- Demo Presentation, [“ScooterLab Demo”](#), [2024 TxDOT Innovation Invitational](#), San Antonio, Texas (July 2024).
- Invited Talk, [“OverHear: Headphone Based Multi-Sensor Keystroke Inference”](#), OU Industrial and Systems Engineering Graduate Seminar Series, University of Oklahoma, Norman, Oklahoma (November 2023).
- Invited Talk, [“Hacklahoma AI Image Generation Workshop”](#), Hacklahoma, University of Oklahoma, Norman, Oklahoma (September 2023).
- Panelist, [“Innovative Assignments with AI”](#), 2023 OU Online Conference, University of Oklahoma, Norman, Oklahoma (August 2023).
- Panel Moderator, [“Wireless and Mobile Security Research and Teaching in the Post-Pandemic World”](#), 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), San Antonio, Texas (May 2022).

PRESS COVERAGE OF RESEARCH

Research covered in 76 press articles across 71 publications in 7 languages — major outlets (Forbes, CBS News, Fast Company), specialized security press, and international media — on work in AI code security, decentralized systems, video-conferencing privacy, micromobility, and smart-device information leakage. Selected items appear below.

AI Code Generation Security

- [“The Threat of Package Hallucinations”](#), *ReversingLabs ConversingLabs Podcast*, June 2025.
- [“A New Threat – Package Hallucination”](#), *I Programmer*, May 2025.
- [“News Roundup – Oracle Plays Breach Word Games, Fast Flux Worries CISA, AI Package Hallucinations, and More”](#), *Packet Pushers (Packet Protector Podcast)*, April 2025.
- [“Why Software Developers Need to Watch Out for Package Hallucinations”](#), *IT Brew*, April 2025.
- [“AI Code Tools Widely Hallucinate Packages”](#), *Dark Reading*, April 2025.
- [“Package Hallucination: LLMs May Deliver Malicious Code to Careless Devs”](#), *Help Net Security*, April 2025.
- [“AI Hallucinations Create ‘Slopsquatting’ Supply Chain Threat”](#), *Infosecurity Magazine*, April 2025.
- [“AI Hallucinations Create a New Software Supply Chain Threat”](#), *SecurityWeek*, April 2025.

- “The Rise of Slopsquatting: How AI Hallucinations Are Fueling a New Class of Supply Chain Attacks”, *Socket*, April 2025.
- “AI Code Helpers Just Can’t Stop Inventing Package Names”, *The Register*, September 2024.
- “AI Threats in Software Development Revealed in New Study”, *EurekAlert!*, April 2025.

Decentralized Systems Security

- “From Oklahoma to Thailand, OU Showcases Blockchain Security Research”, *OU News*, December 2024.

Video Call Keystroke Inference

- “Experts Find a Way to Learn What You’re Typing During Video Calls”, *The Hacker News*, February 2021.
- “Hackers Can Grab Passwords By Watching Your Shoulders Move On Zoom”, *Forbes*, November 2020.
- “This Horrifying Zoom Hack Will Deter You From Ever Side-Chatting Again”, *Fast Company*, November 2020.

E-Scooter Privacy and Security

- “The Great E-Scooter Hack”, *EurekAlert!*, January 2020.

Smart Lighting Information Leakage

- “UTSA Researchers Find Vulnerabilities in Smart Bulbs”, *San Antonio Report*, December 2019.
- “Smarte Glühbirnen: Sicherheitsgefahr”, *Deutschlandfunk Nova*, October 2019.
- “Smart LED Bulbs: Trust but Verify”, *Optics & Photonics News (Optica)*, October 2019.
- “Are ‘Smart’ Light Bulbs a Security Risk?”, *CBS News*, October 2019.
- “Study Warns of Security Gaps in Smart Light Bulbs”, *ScienceDaily*, October 2019.
- “Study Warns of Security Gaps in Smart Light Bulbs”, *Tech Xplore*, October 2019.
- “Novel Attack Technique Uses Smart Light Bulbs to Steal Data”, *BleepingComputer*, August 2018.

AWARDS AND HONORS

- 🏆 USENIX Security Distinguished Paper Award, USENIX Security 2025.
- 🏆 Student Government Association Outstanding Faculty Award, University of Oklahoma, 2023.
- 🏆 Apple Best Paper Award, IEEE WristSense 2018.
- 🏆 Member, Eta Kappa Nu (IEEE-HKN), Epsilon Xi Chapter, 2017.
- 🏆 Dora Wallace Hodgson Outstanding Master’s Thesis Award, Wichita State University, 2015.
- 🏆 Member, Golden Key International Honour Society, 2013.

REFERENCES

- Dr. Shishir Shah, Director, School of Computer Science, University of Oklahoma, Norman, Oklahoma, USA.
sshah@ou.edu · +1 (405) 325-4042
- Dr. Dean Hougen, Professor, School of Computer Science, University of Oklahoma, Norman, Oklahoma, USA.
hougen@ou.edu · +1 (405) 325-3150
- Dr. Murtuza Jadliwala, Associate Professor, Department of Computer Science, University of Texas at San Antonio, San Antonio, Texas, USA.
murtuza.jadliwala@utsa.edu · +1 (210) 458-5693