Nishant Vishwamitra, Ph.D.

864-624-3133 | nishant78255 at gmail dot com | https://business.utsa.edu/faculty/profiles/vishwamitra-nishant.html

Career Objectives

My career objective is to channel my passion for studying *crowdsourcing*, *crisis management*, and *Generative AI in Information Systems*, and addressing issues of *online abuse*, including cyberbullying, cyber harassment, online hate, CSAM and content moderator safety. By combining my dedication to combating these challenges with cutting-edge AI solutions, I aspire to create a safer and more inclusive digital environment for all.

Research Interests

- Crowdsourcing and Crisis Management
- Online Abuse Defense
- Artificial Intelligence (AI) Security
- Generative AI and Large Language Models
- Security and Privacy in Online Social Networks

Professional Experience

University of Texas at San Antonio — San Antonio, TX
Assistant Professor — *August 2022 – Present*
- Department of Information Systems and Cyber Security

University at Buffalo, SUNY — Buffalo, NY
Research Assistant — *June 2020 – June 2022*
- Department of Computer Science and Engineering

Clemson University — Clemson, SC
Research Assistant — *August 2015 – May 2020*
- School of Computing

Education

University at Buffalo, SUNY — Buffalo, NY
Ph.D. in Computer Science and Engineering — *August 2020 – June 2022*
- Advisor: Prof. Hongxin Hu
- Dissertation: Cyber-harassment Framework in Online Social Networks
- GPA: 4.00/4.00

Clemson University — Clemson, SC
Graduate Study in Computer Science — *August 2015 – May 2020*
- Advisor: Prof. Hongxin Hu
- GPA: 3.66/4.00

Visvesvaraya Technological University — Bangalore, India
Bachelor of Engineering in Electronics and Communication — *September 2007 – May 2011*

Research Experience

Crowdsourcing, Crisis Management and Generative Artificial Intelligence

- Explored how socio-cognitive influences, like affective polarization, can systematically distort crowdsourced ground truth in event-centric data through identifiable subgroups [2].
- Studied under what conditions could LLMs replace crowd volunteers in crisis messages categorization [3].
- Examined how prompting LLMs to produce creative outputs impacts the occurrence of hallucinations in the context of generating product descriptions, a type of artistic work in retail [28].
- Studying LLMs prioritization in the context of crisis messages [29].
- Studying algorithmic aversion in the context of protective Artificial Intelligence for photo privacy [32].
- Studying how linguistic consistency and LLM encoders could be leveraged to detect machine-generated text [6, 30].

Online Abuse Defense

- We design a novel system to detect new waves of online hate that performs a reasoning-based decision-making with only a few samples. [4]
- We design a novel methodology to flag down unsafe childrens' games promotion on social media platforms. [5]
- Discovered key vulnerabilities in state-of-the-art unsafe image detectors against adversarial unsafe images. Proposed a novel approach to defend against adversarial unsafe images. Our work has important implications on helping online content moderators, by reducing the mental stress of looking at disturbing images. [8]
- Who are the targets of COVID-19-related online hate? We answer this question by conducting a large-scale study on over 4 million COVID tweets. [10]
- Based on NLP techniques, we detect warning signs during COVID: fixation, group identification, and energy bursts using data from Twitter and Reddit. [11]
- Can machine learning be used to detect the file types of files in encrypted data containers? We answer this question by collecting a large dataset of five file types, conduct EFA to learn whether there are patterns in the data, conduct a large-scale measurement of ML algorithms and propose a system to flag suspicious files. Our system will be used by law enforcement agents to flag encrypted illegal content, such as CSAM. [31]
- Proposed factors of COVID-19 related multimodal Hateful Memes and measurement analysis of the detection capability of multimodal models on COVID-19 related Hateful Memes. [9]
- Proposed novel methodology for the discovery of image-based Cyberbullying related factors and designed multimodal AI for its detection. [15]
- Designed novel explanation method of BERT (a transformer-based model) attention, and discovered novel COVID-19 related hate keywords in Twitter. [16, 18]
- Explored cyberbullying defense using AI in mobile devices. [24]

Privacy and Security in Online Social Networks

- Conducted studies on how crowds validate ground truth data in crisis situations [2]
- Conducted studies on the effect of AI granularity on trust, data mining concerns and AI aversion [32]
- Designed a novel system for enabling automatic, content-based photo privacy management in a user-specific manner in Online Social Networks based on Collaborative Filtering AI [13]
- Developed a taxonomy of obfuscation techniques for content-level photo privacy management in Online Social Networks. [19, 21]
- Proposed a novel access control model for photo sharing in Online Social Networks based on protection of Personally Identifiable Information (PII) items. [23]

Adversarial Attacks on AI Systems

- Proposed Multimodal Decoupling Attacks (MDA) framework to study the adversarial robustness of multimodal AI [12]

Publications (* Denotes High School Students Advised by Me)

[1] **Nishant Vishwamitra**, Ebuka Okpala, Mohammed Aldeen, Pranav Silimkhan, Song Liao, Keyan Guo, Sandeep Shah, Yongkai Wu, Hongxin Hu, Xiaohong Yuan and Long Cheng. AI-Cybersecurity Education Through Designing AI-based Cyberharassment Detection Lab. In *Journal of The Colloquium for Information Systems Security Education*, 2024.

[2] Dan Pienta, Sriram Somanchi, **Nishant Vishwamitra**, Nicholas Berente and Jason Thatcher. Do Crowds Validate False Data? Systematic Distortion and Affective Polarization. ***Management Information Systems Quarterly (MISQ)*** **(ABS 4* Level, JCR Impact Factor 4.373, Financial Times 50)**.

[3] Hrishitva Patel, **Nishant Vishwamitra**, Rohit Valecha and H. Raghav Rao. Automating Information Categorization using LLMs in Crisis Mapping Platforms: An Examination of "Requests for Help" during the 2010 Haiti Earthquake (Conditional Accept). **ICIS**, 2024.

[4] **Nishant Vishwamitra**, Keyan Guo, Farhan Tajwar Romit, Isabelle Ondracek, Long Cheng, Ziming Zhao, and Hongxin Hu. Moderating new waves of online hate with chain-of-thought reasoning in large language models. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 177–177. IEEE Computer Society, 2024.

[5] Keyan Guo, Ayush Utkarsh, Wenbo Ding, Isabelle Ondracek, Ziming Zhao, Guo Freeman, **Nishant Vishwamitra** and Hongxin Hu. Moderating Illicit Online Image Promotion for Unsafe User Generated Content Games Using Large Vision Language Models. In *33rd USENIX Security Symposium (USENIX Security 2024)* ***(Top conference in computer security. Known as a "Big 4" Security Conference)***, 2024.

[6] Mazal Bethany, Brandon Wherry, Emet Bethany, **Vishwamitra, Nishant**, Anthony Rios, and Peyman Najafirad. Deciphering Textual Authenticity: A Generalized Strategy through the Lens of Large Language Semantics for Detecting Human vs. Machine-Generated Text. In *33rd USENIX Security Symposium (USENIX Security 2024)* ***(Top conference in computer security. Known as a "Big 4" Security Conference)***, 2024.

[7] Mazal Bethany, Brandon Wherry, **Vishwamitra, Nishant**, and Peyman Najafirad. Image safeguarding: Reasoning with conditional vision language model and obfuscating unsafe content counterfactually. In *Proceedings of the AAAI Conference on Artificial Intelligence* ***(Top conference in Artificial Intelligence.)***, 2024.

[8] Mazal Bethany, Andrew Seong, Samuel Henrique Silva, Nicole Beebe, **Nishant Vishwamitra**, and Peyman Najafirad. Towards targeted obfuscation of adversarial unsafe images using reconstruction and counterfactual super region attribution explainability. In *32nd USENIX Security Symposium (USENIX Security 2023)* ***(Top conference in computer security. Known as a "Big 4" Security Conference)***, 2023.

[9] **Nishant Vishwamitra**, Keyan Guo, Song Liao, Jaden Mu, Zheyuan Ma, Long Cheng, Ziming Zhao, and Hongxin Hu. Understanding and analyzing covid-19-related online hate propagation through hateful memes shared on twitter. In *Proceedings of the International Conference on Advances in Social Networks Analysis and Mining*, pages 103–107, 2023.

[10] Song Liao, Ebuka Okpala, Long Cheng, Mingqi Li, **Nishant Vishwamitra**, Hongxin Hu, Feng Luo, and Matthew Costello. Analysis of covid-19 offensive tweets and their targets. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining* ***(Top conference in AI and data science)***, 2023.

[11] Matthew Costello, **Nishant Vishwamitra**, Song Liao, Long Cheng, Feng Luo, and Hongxin Hu. Covid-19 and sinophobia: Detecting warning signs of radicalization on twitter and reddit. *Cyberpsychology, Behavior, and Social Networking*, 2023.

[12] **Nishant Vishwamitra**, Hongxin Hu, Long Cheng, Feng Luo, and Matthew Costello. "Robustness of multimodal learning in an adversarial setting". *International Conference On Secure Knowledge Management*, 2023.

[13] **Vishwamitra, Nishant**, Yifang Li, Hongxin Hu, Kelly Caine, Long Cheng, Ziming Zhao, and Gail-Joon Ahn. "PrivacyRec: Automated content-based photo privacy recommendations". *Proceedings of the 12th ACM Conference on Data and Application Security and Privacy (CODASPY) 2022*.

[14] Matthew Costello, Long Cheng, Feng Luo, Hongxin Hu, Song Liao, **Vishwamitra, Nishant**, Mingqi Li, and Ebuka Okpala. "COVID-19: A pandemic of anti-asian cyberhate". *Journal of Hate Studies*, 17(1), 2021.

[15] **Vishwamitra, Nishant**, Hongxin Hu, Feng Luo, and Long Cheng. "Towards understanding and detecting cyberbullying in real-world images". In *Proceedings of the 28th Annual* ***Network and Distributed System Security Symposium (NDSS) (Top conference in computer security. Known as a "Big 4" Security Conference, Acceptance rate: 15.2%)***, 2021.

[16] **Vishwamitra, Nishant**, Ruijia Hu*, Feng Luo, Long Cheng, Matthew Costello, and Yin Yang. "On analyzing covid-19-related hate speech using bert attention". In *Proceedings of the 19th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 669–676. IEEE, 2020.

[17] Ruijia Hu*, Wyatt Dorris*, **Vishwamitra, Nishant**, Feng Luo, and Matthew Costello. "On the impact of word representation in hate speech and offensive language detection and explanation". In *Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy (CODASPY)*, pages 171–173, 2020.

[18] Wyatt Dorris*, Ruijia Hu*, **Vishwamitra, Nishant**, Feng Luo, and Matthew Costello. "Towards automatic detection and explanation of hate speech and offensive language". In *Proceedings of the Sixth International Workshop on Security and Privacy Analytics (IWSPA)*, pages 23–29, 2020.

[19] Yifang Li, **Vishwamitra, Nishant**, Hongxin Hu, and Kelly Caine. "Towards a taxonomy of content sensitivity and sharing preferences for photos". In *Proceedings of the 2020 Conference on Human Factors in Computing Systems (****CHI) (Top conference in HCI. Acceptance rate: 24.3%)***, pages 1–14, 2020.

[20] Xiang Zhang, **Vishwamitra, Nishant**, Hongxin Hu, and Feng Luo. "CrescendoNet: A new deep convolutional neural network with ensemble behavior". In *Proceedings of the 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 311–317. IEEE, 2018.

[21] Yifang Li, **Vishwamitra, Nishant**, Bart P Knijnenburg, Hongxin Hu, and Kelly Caine. "Effectiveness and users' experience of obfuscation as a privacy-enhancing technology for sharing photos". *Proceedings of the 20th ACM Conference on Computer-Supported Cooperative Work and Social Computing (****CSCW) (Top conference in HCI)***, 1, 2017.

[22] Yifang Li, **Vishwamitra, Nishant**, Hongxin Hu, Bart P Knijnenburg, and Kelly Caine. Effectiveness and users experience of face blurring as a privacy protection for sharing photos via online social networks. In *Proceedings of the Human Factors and Ergonomics Society (HFES) Annual Meeting*, volume 61, pages 803–807. SAGE Publications Sage CA: Los Angeles, CA, 2017.

[23] **Vishwamitra, Nishant**, Yifang Li, Kevin Wang, Hongxin Hu, Kelly Caine, and Gail-Joon Ahn. "Towards PII-based multiparty access control for photo sharing in online social networks". In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies (SACMAT)*, pages 155–166, 2017.

[24] **Vishwamitra, Nishant**, Xiang Zhang, Jonathan Tong*, Hongxin Hu, Feng Luo, Robin Kowalski, and Joseph Mazer. "MCDefender: Toward effective cyberbullying defense in mobile online social networks". In *Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics (IWSPA)*, pages 37–42, 2017.

[25] Yifang Li, **Nishant Vishwamitra**, Bart P. Knijnenburg, Hongxin Hu, and Kelly Caine. Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 39–47, 2017.

[26] Xiang Zhang, Jonathan Tong*, **Vishwamitra, Nishant**, Elizabeth Whittaker, Joseph P Mazer, Robin Kowalski, Hongxin Hu, Feng Luo, Jamie Macbeth, and Edward Dillon. "Cyberbullying detection with a pronunciation based convolutional neural network". In *2016 15th IEEE international conference on machine learning and applications (ICMLA)*, pages 740–745. IEEE, 2016.

Under Revision

[27] **Nishant Vishwamitra**, Paul Rad, Rohit Valecha and H. Raghav Rao. Examining Structural and Sentimental Inconsistencies:A Corroboration Theory Approach to Fake News Detection. ***Journal of the Association of Information Systems.*** **Status: Under Revision.**

Under Submission

[28] **Nishant Vishwamitra**, Saman Bina, Mazal Bethany, Rohit Valecha and H. Raghav Rao. Assessing Hallucinations When Pursuing Creativity in Large Language Models' Outputs. ***Early Career ISR-INFORMS ISS Workshop.*** **Status: Under Review.**

Selected Working Papers

[29] **Nishant Vishwamitra**, Saman Bina, Ramiro Rodriguez, Rohit Valecha and H. Raghav Rao. How Do LLMs Prioritize Crisis Messages? An Examination of "Requests for Help" during the 2010 Haiti Earthquake. Target: *Management Information Systems Quarterly (MISQ)* Status: Final Iterations.

[30] **Nishant Vishwamitra**, Paul Rad, Rohit Valecha and H. Raghav Rao. Manufactured Deceit: Detection and Characterization of Large-scale AI-generated Disinformation. Target: *Management Information Systems Quarterly (MISQ)* Status: Final Iterations.

[31] Adam Hooker, Wenjian Huang, Shalini Kurumathur, Raymond Choo and **Nishant Vishwamitra**. Towards Understanding and Detecting File Types in Encrypted Data Containers for Law Enforcement Applications. ***ESORICS 2024***.

[32] Pienta D., **Vishwamitra N.**, Thatcher J., A. Johnston, and H Hu. Tell Us Your Secrets: Trust, Data Exfiltration, and Aversion in the Design of Protective Artificial Intelligence. Target: *Management Information Systems Quarterly (MISQ)* Status: Final Iterations.

[33] **Nishant Vishwamitra**, Dan Pienta, Saman Bina and Jeff Donahoo. Sedition Hunting: Addressing Cognitive Biases in Crisis Crowdsourcing by Leveraging Large Vision-Language Models. Target: *Information Systems Research* Status: Working.

[34] Nirmalee I. Raddatz, Dan Pienta, **Vishwamitra, Nishant**, and Jason Thatcher. "AI Transparency and Interpretability Study". Target: *Management Science Special Issue on The Human-Algorithm Connection* Status: Working.

[35] **Vishwamitra, Nishant**, Nirmalee I. Raddatz, Dan Pienta, and Jason Thatcher. AI Fairness Study. Target: *Management Information Systems Quarterly (MISQ) Special Issue on Digital Technologies and Social Justice* Status: Final Iterations.

Poster Presentations

[36] **Vishwamitra, Nishant**. AutoPri: Collaborative Photo Privacy in Online Social Networks. *AI for IndustryConference, CUiCAR, Greenville SC*, 2018.

Leadership/Supervision Experience

Colloquium Coordinator August 2023 – Present
UTSA *San Antonio, TX*

- Inviting and hosting speakers for the AT&T Distinguished Speaker Series.
- Organize poster session for our PhD students.

DEFCON Self-Driving Capture the Flag (CTF) 2021 July 2021 – August 2021

University at Buffalo, SUNY *Buffalo, NY*

- Led a team of four Ph.D. students and one graduate student in the DEFCON Autodriving CTF challenge. Overall, over 100 teams participated in this event all over the world.
- Our team **finished 5^{th}** in this challenge overall, and **1^{st}** in USA.
- We **finished 1^{st}** all over the world in the Lane Detection challenge, a task fully handled by me.

AI Cybersecurity Labs Development June 2021 – Present

University at Buffalo, SUNY *Buffalo, NY*

- Leading the design of the NSF funded AI Cybersecurity Labs, a suite of labs to train students in AI security issues.
- The labs are currently used as part of the course curriculum in Clemson University and North Carolina A&T University.
- Multiple talks were given at the GenCyber 2021 event hosted in North Carolina A&T University about the labs.
- Link: https://colab.research.google.com/drive/1dmwP_N7fkqZIbPVInb2XBgF4NnMUX1-p?usp=sharing

UB Cybersecurity Research Lab Paper Presentations August 2020 – Present

University at Buffalo, SUNY *Buffalo, NY*

- Led the initiative of weekly paper presentations, where each student in the lab presents and discusses research papers published in top cybersecurity and AI conferences.
- An important outcome of this initiative is our paper reading group list, a repository of all the research papers and talk videos.

Co-supervision of Incoming Students Dec. 2019 – Present

University at Buffalo, SUNY *Buffalo, NY*

- As part of my Ph.D. studies, I co-supervised multiple incoming students.
- Led Zheyuan Ma (UB Ph.D, 2021) and Anoosha Seelam (UB MS, 2020) in the analysis and measurement of COVID-19 related Hateful Memes.
- Mentored Rui Cao (Clemson University MS, 2020) in design and development of a robustness analysis framework for Multimodal AI.
- Mentored Roger Hu (Duke University BS, 2021) and Wyatt Dorris (Clemson University BS, 2021), **two high school students** from the D.W. Daniel High School, Clemson, in two research papers published at ICMLA 2021 and IWSPA 2020 on explanation and detection of hateful tweets.

Host of Graduate Student Roundtable Meetings Dec. 2019 – Present

University at Buffalo, SUNY *Buffalo, NY*

- I regularly host the graduate student roundtable meetings, held as part of the CSE department faculty hiring process.
- These meetings are crucial for the incoming faculty members to know about various research activities in the department, and also for graduate students to know about the research objectives of incoming faculty.

Grants

CAREER: Towards Building Foundation Models for Online Abuse Defense San Antonio, TX

Sponsoring Agency: National Science Foundation *2025 – 2030*

- Status: Under Review
- Award Amount: $618,273
- This project proposes foundational model, educational materials and outreach activities for defending against online abuse.
- I am the **PI** of the grant.

Collaborative Research: SaTC: EDU: SecGAI: Advancing Generative AI Security Education through Cutting-Edge Research Integration & Culturally Relevant Pedagogy San Antonio, TX

Sponsoring Agency: National Science Foundation *2025 – 2028*

- Status: Under Review
- Award Amount: $300,000

- This project proposes an educational platform, hands-on labs, and curriculur material for Generative AI cybersecurity education.
- I am the **PI** of the grant.

AbuseFound: Towards Foundation Models for Online Abuse Defense San Antonio, TX
Sponsoring Agency: Google Research *2025 – 2026*

- Status: Under Review
- Award Amount: $100,000
- This project proposes foundational model for online abuse defense.
- I am the **PI** of the grant.

Enhancing Collaborative Sensemaking in Digital Sleuthing Through Social Media Analysis and Automated Image Triage San Antonio, TX
Sponsoring Agency: UTSA FY25 Internal Research Awards (INTRA) Seed Grant program *2025 – 2026*

- Status: Awarded
- Award Amount: $5,000
- This project proposes an educational platform, hands-on labs, and curricular material for Generative AI cybersecurity education.
- I am the **PI** of the grant.

NSF CRII: SaTC: Towards Understanding and Defending Against New Waves of Online Hate San Antonio, TX
Sponsoring Agency: National Science Foundation *2023 – 2024*

- Status: Awarded
- Award Amount: $175,000.00
- This project is studying new waves of online hate and the spread of cross-platform hate on Internet platforms.
- I am the **PI** of the grant.

Collaborative Research: Education DCL: EAGER: SecGAI: Learning Platform and Curriculum Development for Socially Secure Generative AI San Antonio, TX
Sponsoring Agency: National Science Foundation *2023 – 2024*

- Status: Declined
- Award Amount: $300,000.00
- This project proposes a new educational platform to train students on the social cybersecurity threats of Generative AI.
- I am the **PI** of the grant.

FW-HTF-RL: Preparing for the next Digital Divide: Upskilling Workers in the New Era of Artificial Intelligence San Antonio, TX
Sponsoring Agency: National Science Foundation *2023 – 2027*

- Status: Declined
- Award Amount: $1,698,604.00
- This research aims to develop an innovative data base from multiple sources including Patent, ONET and BLS databases to help extract future work core competency and identify key associated skills that are needed by future workers.
- I am the **Co-PI** of the grant. PI: Raghav Rao, UTSA.

Why do crowds validate false data? Systematic errors in validating crowdsourced ground truth during a crisis Waco, TX
Sponsoring Agency: Baylor University Research Committee ONE-URC Program *June 2021 – May, 2022*

- Status: Granted
- Award Amount: $4,500.00
- This project focuses on studying why crowds validate fake information online using eye-tracking studies.
- I am the **Co-PI** of the grant. PI: Dan Pienta, UTK.

Teaching Experience

Assistant Professor Aug. 2022 – Present

The University of Texas at San Antonio *San Antonio, TX*

- Teacher for the following courses
  - IS-6733 Deep Learning on Cloud Platforms, Fall 2024
  - IS-6733 Deep Learning on Cloud Platforms, Spring 2024
  - IS-3423 Network Security, Fall 2022
  - IS-3423 Network Security, Spring 2023
  - IS-3423 Network Security, Fall 2023
- My responsibilities included
  - Instructor in-charge for lectures and hands-on labs in all formats

Graduate Teaching Assistant (TA) Jan. 2017 – Jan. 2020

Clemson University *Clemson, SC*

- Teaching assistant for the following courses
  - CPSC-8580 Security in Emerging Systems, Fall 2020
  - CPSC-8580 Security in Emerging Systems, Fall 2019
  - CPSC-8580 Security in Emerging Systems, Fall 2018
  - CPSC-6200 Computer Security Principles, Fall 2018
  - CPSC-4200 Computer Security Principles, Fall 2018
  - CPSC-8580 Security in Emerging Systems, Spring 2018
  - CPSC-6200 Computer Security Principles, Fall 2017
  - CPSC-4200 Computer Security Principles, Fall 2017
  - CPSC-8570 Network Technologies Security, Spring 2017
- My TA responsibilities included
  - Instructor in-charge for cyber security labs
  - Designing and grading hands-on cyber security labs
  - Answer students' questions about lab tasks, troubleshoot student issues, and help students' setup lab environment
  - Grading assignments, quizzes, exams and other submissions
  - Filling-in for the instructor for face-to-face course lectures
- The cyber security labs designed for courses are listed below
  - Content-level photo privacy management (CPSC 8580, CPSC 6200, CPSC 4200)
  - Hacking deep learning models (CPSC 8580)

Additional Experience

System Engineer Jun. 2011 – Aug. 2015

Infosys Technologies Ltd. *Bangalore, India*

- Designed a web application for a leading banking company.
- The application is used by bankers for book-keeping of on-going projects.
- Worked with a large team from multiple locations.

Collaborators

- Information Systems
  - Daniel Pienta, Assistant Professor at University of Tennessee, Knoxville (MISQ [2, 32, 34])
  - Jason Thatcher, Professor at Temple University (MISQ [2, 32, 34])
  - Nicholas Berente, Professor at University of Notre Dame (MISQ [2])
  - Raghav Rao, Professor at UTSA ([30])
  - Raymond Choo, Professor at UTSA ([31])
  - Nicole Beebe, Professor at UTSA ([8])
  - Rohith Valecha, Associate Professor at UTSA ([30])
  - Allen Johnston, Professor at University of Alabama (MISQ [32])
  - Nirmalee Raddatz, Assistant Professor at The University of Memphis (MISQ Special Issue on Digital Technologies and Social Justice [34])
  - Sriram Somanchi, Assistant Professor at University of Notre Dame (MISQ [2])

- Saman Bina, Assistant Professor at Baylor University ([33])

- Computer Science
  - Ziming Zhao, Assistant Professor at SUNY Buffalo (AAAI [12])
  - Feng Luo, Professor at Clemson University (NDSS [15], AAAI [12], ICMLA [16], CODASPY [17])
  - Long Cheng, Assistant Professor at Clemson University (NDSS [15], AAAI [12], ICMLA [16], CODASPY [17])
  - Paul Rad, Associate Professor at UTSA (USENIX Security [8])

- HCI and Social Science
  - Kelly Caine, Associate Professor at Clemson University (CHI [19], CSCW [21], SACMAT [23])
  - Matthew Costello, Assistant Professor at Clemson University (ICMLA [15], CODASPY [17])

Media and News

- I have appeared on multiple media outlets such as *WIRED*, *KEN5 News*, *CBS*, and *News4SA* to discuss Generative AI security issues.
- I am a **TEDxSanAntonio** speaker for 2024's Compassion, Caring, and Community Salon, held on Saturday, May 18th, 2024.
- My NSF CRII award featured on ***UTSA Alvarez College of Busines News***. Article Link: https://business.utsa.edu/nishant-vishwamitra-nsf-grant/
- My paper on image-based cyberbullying accepted at NDSS [15] was reported on ***SUNY Buffalo CSE News***. Article Link: https://engineering.buffalo.edu/computer-science-engineering/news-and-events/news.host.html/content/shared/engineering/home/articles/news-articles/2021/cybersecurity-research-showcased-at-network-and-distributed-system-security-symposium.detail.html
- My work on content-level photo privacy protection [23] was reported in ***Clemson IDEAS magazine***. Article Link: https://cecas.clemson.edu/ideas/archives/spring20/. Video Link: https://www.youtube.com/watch?v=n2Hnvc8xcX4
- My paper on online hate speech detection and understanding [18] with two high school students has been reported in ***Clemson Newsstand***. Article Link: https://news.clemson.edu/artificial-intelligence-could-help-stem-the-tide-of-online-hate-speech-clemson-university-researchers-say/
- My work on image-based cyberbullying was shared by the NDSS Symposium on ***Twitter***. Link: https://twitter.com/NDSSSymposium/status/1364666537559298048?s=20

Invited Talks

- **Great Lakes Security Day 2021.** I am invited to talk on visual cyberbullying threat and defenses at Great Lakes Security Day (GLSD) 2021, on November 12^{th}2021. GLSD brings together premier practitioners, researchers, students, and funding partners in security, to share latest advances, debate roadmaps and future directions, create new collaborations, and seek new opportunities in cybersecurity, in and around Western and Upstate New York.
- **GenCyber 2021 at North Carolina A&T University.** I was invited to talk on AI-related cybersecurity challenges and cyberbullying defense at the GenCyber 2021 event at North Carolina A&T University, during two sessions held on July 21^{st}2021, and July 28^{th}2021. The GenCyber 2021 was attended by **60+ high school students** and teachers in a 2-week summer camp centered on cyber security education.
- **UpBeat at SUNY Buffalo, CSE Department.** I was invited to talk on visual cyberbullying defense at UpBeat, organized by the CSE department at SUNY Buffalo on October 1^{st}2021. The UpBeat is a weekly event attended by faculty and graduate students to learn about ongoing research projects in the department.

Technical Program Committee

Guest Editor
- Information Systems Frontiers

Program Committee
- 10th ACM International Workshop on Security and Privacy Analytics (IWSPA 2024), Porto, Portugal

Conference Committee
- Annual Computer Security Applications Conference (ACSAC) Artifacts Evaluation Committee, 2021
- IEEE International Workshop Big Data Security and Services (BigDataService), 2018–2020

Poster Committee
- Poster Program of ACM Conference on Data and Application Security and Privacy (CODASPY), 2018–2020

Conference Paper Reviewer

- The Fourteenth International Conference on Advances in Computer-Human Interactions (ACHI), 2021
- International Conference On Design Science Research In Information Systems And Technology (DESRIST), 2021
- International Workshop on Automotive and Autonomous Vehicle Security (AutoSec), 2021
- The Web Conference (WWW), 2021
- ACM Conference on Computer and Communications Security (CCS), 2018–2021
- ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2018–2021
- Annual Computer Security Applications Conference (ACSAC), 2018–2021
- ACM Conference on Data and Application Security and Privacy (CODASPY), 2018–2020
- ACM Symposium on Access Control Models and Technologies (SACMAT), 2018–2020
- IEEE Conference on Communications and Network Security (CNS), 2018–2021
- IEEE International Conference on Computer Communications and Networks (ICCCN), 2018–2020
- ACM SIGCOMM Workshop on Security in Softwarized Networks: Prospects and Challenges (SecSoN), 2018
- ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (SDN-NFV Security), 2017–2020
- International Conference on Information and Communications Security (ICICS), 2018–2020
- International Conference on Privacy, Security and Trust (PST), 2018–2020
- IEEE International Conference on Cloud Networking (CloudNet), 2018–2020
- IEEE International Conference on Smart City Innovations (SCI), 2018–2021-0

Conference Track Chairing

- Hawaii International Conference on System Sciences (HICSS) 2024, SJ – Criminal Justice mini-track chair with Dan Pienta and Raymond Choo, 2024 – 2025

Journal Paper Reviewer

- Transactions on Dependable and Secure Computing (TDSC), 2017–2020
- Transactions on Information Forensics & Security (TIFS), 2018–2020

Honors And Awards

- Talford family fellowship for cyber security research, 2018

Technical Skills

Languages: Python, C/C++, Latex, JavaScript, HTML/CSS, R
Frameworks: PyTorch, Tensorflow
Developer Tools: Git, Vim, Eclipse
Libraries: Pandas, NumPy, Matplotlib
MOOC: Deep Learning by deeplearning.ai on Coursera (January 15, 2019)