VISHNU ASUTOSH DASU

Google Scholar ⋄ GitHub ⋄ LinkedIn ⋄ vdasu@psu.edu ⋄ +1 (582) 203-9641 ⋄ vdasu.github.io

EDUCATION

- **Pennsylvania State University** *Aug 2024 - May 2028*
  Doctor of Philosophy, Computer Science and Engineering
  - *Research Area*: Trustworthy AI and Software Security
  - *Advisor*: Prof. Gang (Gary) Tan
- **Pennsylvania State University** *Aug 2022 - May 2024*
  Master of Science, Computer Science and Engineering
  - *Thesis*: "Mitigating Unfairness in Deep Learning"
  - *Advisor*: Prof. Gang (Gary) Tan
- **Manipal Institute of Technology (MIT), Manipal** *July 2016 - July 2020*
  Bachelor of Technology, Computer Science and Engineering

SELECTED PUBLICATIONS

* - Equal Contribution/Alphabetical Order

- **Attention Pruning: Automated Fairness Repair of Language Models via Surrogate Simulated Annealing [pdf]**
  48th International Conference on Software Engineering (ICSE), 2026
  Vishnu Asutosh Dasu, Md Rafi ur Rashid, Vipul Gupta, Saeid Tizpaz-Niari, Gang Tan
- **Improving Noise Efficiency in Privacy-preserving Dataset Distillation [pdf]**
  International Conference on Computer Vision (ICCV), 2025
  Runkai Zheng, **Vishnu Asutosh Dasu**, Yinong Wang, Haohan Wang, Fernando De la Torre
- **Privacy-Preserving Data Deduplication for Enhancing Federated Learning of Language Models [pdf]**
  Network and Distributed System Security (NDSS) Symposium, 2025
  Aydin Abadi*, **Vishnu Asutosh Dasu***, Sumanta Sarkar*
- **NeuFair: Neural Network Fairness Repair with Dropout [pdf]**
  33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA), 2024
  Vishnu Asutosh Dasu, Ashish Kumar, Saeid Tizpaz-Niari, Gang Tan
- **Impact of Data Duplication on Deep Neural Network-Based Image Classifiers: Robust vs. Standard Models [pdf]**
  IEEE Deep Learning Security and Privacy Workshop (DLSP), IEEE S&P, 2025
  Alireza Aghabagherloo, Aydin Abadi, Sumanta Sarkar, **Vishnu Asutosh Dasu**, Bart Preneel
- **PROV-FL: Privacy-preserving Round Optimal Verifiable Federated Learning [pdf]**
  15th ACM Workshop on Artificial Intelligence and Security (AISEC), ACM CCS, 2022
  Vishnu Asutosh Dasu, Sumanta Sarkar, Kalikinkar Mandal
- **Side Channel Attack On Stream Ciphers: A Three-Step Approach To State/Key Recovery [pdf]**
  IACR Conference on Cryptographic Hardware and Embedded Systems (CHES), 2022
  Satyam Kumar, **Vishnu Asutosh Dasu**, Anubhab Baksi, Santanu Sarkar, Dirmanto Jap, Jakub Breier, Shivam Bhasin
- **New Results on Machine Learning-Based Distinguishers [pdf]**
  IEEE Access, 2023

Anubhab Baksi*, Jakub Breier*, **Vishnu Asutosh Dasu***, Xiaolu Hou*, Hyunji Kim*, Hwajeong Seo*

- **Three Input Exclusive-OR Gate Support For Boyar-Peralta's Algorithm [pdf]**
  22nd International Conference on Cryptology in India (Indocrypt), 2021
  Anubhab Baksi, **Vishnu Asutosh Dasu**, Banashri Karmakar, Anupam Chattopadhyay, Takanori Isobe

- **LIGHTER-R: Optimized Reversible Circuit Implementation For SBoxes**
  32nd IEEE International System-on-Chip Conference (SOCC), 2019
  Vishnu Asutosh Dasu, Anubhab Baksi, Sumanta Sarkar, Anupam Chattopadhyay

PREPRINTS/UNDER SUBMISSION

- **Trust Me, I Can Handle It: Self-Generated Adversarial Scenario Extrapolation for Robust Language Models [pdf]**
  (Under Review) The 40th Annual AAAI Conference on Artificial Intelligence (AAAI), 2026
  Md Rafi Ur Rashid, **Vishnu Asutosh Dasu**, Ye Wang, Gang Tan, Shagufta Mehnaz

- **Finding Probabilistic Sub-invariants via Search Space Algorithms under Noisy Cost Functions**
  (Under Review) 32nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), 2026
  Ashish Kumar, **Vishnu Asutosh Dasu**, Saied Tizpaz-Niari, Gang Tan

- **Scalable Privacy-preserving Federated K Nearest Neighbors**
  (Under Submission) 46th IEEE Symposium on Security and Privacy (S&P)
  Aydin Abadi*, **Vishnu Asutosh Dasu***, Sumanta Sarkar*

- **Gradient-Free Privacy Leakage in Federated Language Models through Selective Weight Tampering [pdf]**
  Md Rafi Ur Rashid, **Vishnu Asutosh Dasu**, Kang Gu, Najrin Sultana, Shagufta Mehnaz

- **iResolveX: Multi-Layered Indirect Call Resolution via Static Reasoning and Learning-Augmented Refinement**
  (Under Submission) 46th IEEE Symposium on Security and Privacy (S&P)
  Monika Santra, Bokai Zhang, Mark Lim, **Vishnu Asutosh Dasu**, Dongrui Zeng, Gang Tan

ACADEMIC AND WORK EXPERIENCE

- **Pennsylvania State University** *Aug. 2022 - Present*
  Graduate Research/Teaching Assistant *Advisors: Gang Tan, Saeid Tizpaz-Niari, Shagufta Mehnaz*
  - *Projects:* Data extraction attacks on federated LLMs, Trustworthy Code Generation LLMs, Fairness and Robustness of LLMs, Binary Analysis, Software Security

- **Tata Research Development and Design Centre (TRDDC)** *Sept 2020 - June 2022*
  Researcher, Cybersecurity and Privacy *Advisors: Sumanta Sarkar*
  - *Projects:* Privacy-preserving Federated Learning, Secure Multiparty Computation, Insider Threat Detection

- **Citrix R&D** *Jan 2020 - June 2020*
  Software Engineer Intern, Citrix Analytics for Security (CAS)
  - Full-stack Web Developer (Spring Boot, React.js)

- **Nanyang Technological University (NTU)** *Dec 2019 - Jan 2020*
  Research Intern *Advisors: Anupam Chattopadhyay*

  - *Projects:* Optimizing hardware implementations of block ciphers

- **Tata Consultancy Services (TCS) Research** *May 2019 - July 2019*
  Research Intern, Cybersecurity and Privacy *Advisors: Chalamala Srinivasa Rao*
  - *Projects:* Adversarial attacks and defenses on Convolution Neural Networks (CNNs)

- **Tiny Banyan Technologies** *Feb 2019 - May 2019*
  Machine Learning Intern
  - *Projects:* Real-time detection of humans and firearms from CCTV footage using deep learning

- **Indian Statistical Institute** *May 2018 - July 2018*
  Summer Scholar *Advisors: Dipti Prasad Mukherjee*
  - *Project:* 3-D coordinate estimation of humans from 2-D live video feed

SKILLS

- **Languages:** Python, C/C++, Java, Rust, HTML/CSS, Go, JavaScript, SQL
- **AI/ML Expertise:** Machine Learning, Deep Learning, Large Language Models (LLMs), Trustworthy AI (Fairness, Privacy, Robustness), NLP, Computer Vision
- **Tools:** PyTorch, TensorFlow, Huggingface, GMP, OpenSSL, LaTeX, KLEE, LLVM, Angr, Git
- **Areas of Expertise:** Software & Hardware Security, Privacy, Applied Cryptography

SERVICE

- **Reviewer:** AAAI 2026, IEEE TIFS (2025), IEEE Access (2025)
- **Artifact Evaluation Committee:** ACM CCS 2025
- **External Reviewer:** NDSS 2025, OOPSLA 2025, IEEE S&P 2025
- **Organizer:** Penn State Security Reading Group (2024 - Present)
- **Judge:** Penn State Undergraduate Exhibition 2025

AWARDS AND ACHIEVEMENTS

- **Distinguished Reviewer Award**: Received the distinguished reviewer award for artifact evaluation in ACM CCS 2025.
- **Student Travel Grant**: Received the travel grant to attend ICCV 2025.
- **Internet Society Fellowship**: Received the Internet Society Fellowship to attend NDSS 2025.
- **TCS Citation Award** *(3× recipient)*: Received the award for outstanding contribution to TCS.
- **Scholarship**: Received a scholarship to attend the *Winter School on Responsible AI* in Israel.
- **Best Project Award**: Received the Best Project Award during the *Fifth Summer School on Computer Vision, Graphics and Image Processing*, Indian Statistical Institute (ISI) Kolkata.
- **IGVC**: Placed 2^{nd} in the Interoperability Profiles Challenge and 9^{th} overall at *Intelligent Ground Vehicle Competition (IGVC)* 2018. Second-best among all teams from India.
- **DAGsHub Award:** Received a $500 award from *DAGsHub* for completing the *ML Reproducibility Challenge Spring 2021.*

PROFESSIONAL MEMBERSHIPS

- Student Member of the ACM
- Student Member of IEEE