VISHNU ASUTOSH DASU

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

EDUCATION

- **Pennsylvania State University** *Aug 2024 - May 2027*
  Doctor of Philosophy, Computer Science and Engineering CGPA: 3.92/4
  – *Advisor*: Prof. Gang (Gary) Tan
  – *Research Area*: Trustworthy Machine Learning and Software Security
- **Pennsylvania State University** *Aug 2022 - May 2024*
  Master of Science, Computer Science and Engineering CGPA: 3.92/4
  – *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 CGPA: 8.71/10
  – *Minor in Big Data*

SELECTED PUBLICATIONS *Citations: 118, h-index: 6*

* - Equal Contribution/Alphabetical Order

- **Privacy-Preserving Data Deduplication for Enhancing Federated Learning of Language Models**
  Conditionally Accepted at Network and Distributed System Security (NDSS) Symposium, 2025
  Aydin Abadi*, **Vishnu Asutosh Dasu***, Sumanta Sarkar*
- **NeuFair: Neural Network Fairness Repair with Dropout**
  33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA)
  Vishnu Asutosh Dasu, Ashish Kumar, Saeid Tizpaz-Niari, Gang Tan
- **FLTrojan: Privacy Leakage Attacks against Federated Language Models Through Selective Weight Tampering**
  Pre-print on arXiv and under review at IEEE EuroS&P, 2025
  Md Rafi ur Rashid, **Vishnu Asutosh Dasu**, Kang Gu, Najrin Sultana, Shagufta Mehnaz
- **PROV-FL: Privacy-preserving Round Optimal Verifiable Federated Learning**
  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**
  IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), 2022
  Satyam Kumar, **Vishnu Asutosh Dasu**, Anubhab Baksi, Santanu Sarkar, Dirmanto Jap, Jakub Breier, Shivam Bhasin
- **EvoquerBot: A multimedia chatbot leveraging synthetic data for cross-domain assistance**
  Alexa Prize TaskBot Challenge 2 Proceedings
  Team EvoquerBOT, Penn State University
- **New Results on Machine Learning-Based Distinguishers**
  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**
  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

ACADEMIC AND WORK EXPERIENCE

- **Pennsylvania State University** *Aug. 2022 - Present*
  Graduate Research/Teaching Assistant *University Park, PA, USA*
  – *Supervisors:* Prof. Gary Tan, Prof. Saeid Tizpaz-Niari, & Prof. Shagufta Mehnaz
  – *Projects:* Private data extraction attacks on federated LLMs, Trustworthy Code Generation LLMs, Fairness of LLMs and Machine Learning
- **Tata Consultancy Services (TCS) Research** *Sept 2020 - June 2022*
  Researcher, Cybersecurity and Privacy *Bangalore, India*
  – *Supervisors:* Prof. Sumanta Sarkar & Manish Shukla
  – *Project:* Privacy-preserving federated learning, Insider threat detection from network logs
- **Citrix R&D** *Jan 2020 - June 2020*
  Software Engineer Intern, Citrix Analytics for Security (CAS) *Bangalore, India*
  – Full-stack Web Developer
- **Nanyang Technological University (NTU)** *Dec 2019*
  Research Intern *Singapore*
  – *Supervisor:* Prof. Anupam Chattopadhyay
  – *Project:* Optimized hardware implementations of block ciphers
- **TCS Research** *May 2019 - July 2019*
  Research Intern, Cybersecurity and Privacy *Hyderabad, India*
  – *Supervisor:* Dr. Chalamala Srinivasa Rao
  – *Project:* Adversarial attacks and defenses on Convolution Neural Networks (CNNs)
- **Tiny Banyan Technologies** *Feb 2019 - May 2019*
  Machine Learning Intern *Remote*
  – *Project:* Real-time detection of humans and firearms from CCTV footage using deep learning
- **Indian Statistical Institute** *May 2018 - July 2018*
  Summer Scholar *Kolkata, India*
  – *Supervisor:* Prof. Dipti Prasad Mukherjee
  – *Project:* 3-D coordinate estimation of humans from 2-D live video feed
- **Project Manas (AI Robotics)** *Feb 2018 - Feb 2019*
  – *Projects:* Clustering and tracking LIDAR point clouds, Sensor fusion using Kalman Filters

SKILLS

- **Beginner:** Go, Rust, Swift, iOS Development, Android Development
- **Intermediate:** C++, Java, Javascript, HTML, Cryptography, SQL, Web Development, Computer Vision, Image Processing, Natural Language Processing, Robotics, ROS, Git, Linux
- **Advanced:** Machine Learning, Deep Learning, Trustworthy ML, Python, C, LaTeX, Security, Privacy

SERVICE

- **Organizer**, Penn State Security Reading Group *2024*
- **External Reviewer**, Network and Distributed System Security (NDSS) Symposium *2025*
- **Reviewer**, ReScience *Present*

AWARDS AND ACHIEVEMENTS

- **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.
- **ACM ICPC Regionals**: Represented MIT Manipal at the 2017 *ACM ICPC Asia Regional Contest.*
- **DAGsHub Award:** Received a $500 award from *DAGsHub* for completing the *ML Reproducibility Challenge Spring 2021.*