VISHNU ASUTOSH DASU

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

EDUCATION

- **The Pennsylvania State University** *Aug 2022 - May 2024*
  Master of Science, Computer Science and Engineering CGPA: 3.95/4
  – Thesis: "Mitigating Unfairness in Deep Learning"
- **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.

ACADEMIC AND WORK EXPERIENCE

- **OpenMined Research** *Aug 2023 - Present*
  Researcher *Remote*
  – Working on analyzing and preventing privacy risks in large language models.
- **The Pennsylvania State University** *May 2023 - July 2023*
  Graduate Research Assistant *University Park, PA, USA*
  – Working on mitigating unfairness deep learning models to improve utility on socioeconomic scenarios.
  – Developed a algorithm to "repair" neurons in neural networks to improve fairness.
- **The Pennsylvania State University** *Jan 2023 - May 2023*
  Graduate Research Assistant *University Park, PA, USA*
  – Worked on the NLP team of *EvoquerBOT* for the Amazon Alexa Prize Taskbot Challenge.
  – Developed language models and data pre-processing techniques for conversational task assistants.
- **Tata Consultancy Services (TCS) Research** *Sept 2020 - June 2022*
  Researcher, Cybersecurity and Privacy *Bangalore, India*
  – Worked on anomaly and insider threat detection using ML. Developed a framework to detect suspicious IPs in an enterprise from network logs using autoencoders.
  – Worked on privacy-preserving ML and developed a single-round, fault-tolerant secure aggregation protocol for federated learning with differential privacy guarantees.
- **Citrix R&D** *Jan 2020 - June 2020*
  Software Engineer Intern, Citrix Analytics for Security (CAS) *Bangalore, India*
  – Worked as a full-stack developer in the App Platform team of Citrix Analytics for Security (CAS).
  – Developed interactive dashboards for analyzing sensitive data to identify malicious user behavior in an enterprise.
  – Developed and implemented a trust service to validate API calls to prevent malicious and unauthorized requests.
- **Nanyang Technological University (NTU)** *Dec 2019*
  Research Intern *Singapore*
  – Developed algorithms and tools to generate optimized ASIC implementations of block ciphers.
  – Generated the best-known implementation of the `AES MixColumn` matrix using 12 XOR2 and 47 XOR3 gates.
- **TCS Research** *May 2019 - July 2019*
  Research Intern, Cybersecurity and Privacy *Hyderabad, India*
  – Worked on explainable artificial intelligence and defenses against white-box adversarial attacks.
  – Developed an algorithm using denoising autoencoders to remove FGSM and PGD adversarial noise added to RGB images.
- **Tiny Banyan Technologies** *Feb 2019 - May 2019*
  Machine Learning Intern *Remote*
  – Developed deep learning models to detect humans and firearms from CCTV footage.
  – Worked on all stages of the ML lifecycle, starting from data collection, labeling, analysis, model design, and training.

- **Indian Statistical Institute** *May 2018 - July 2018*
  Summer Scholar *Kolkata, India*
  - Worked on image processing and computer vision for human detection from live video feeds.
  - Developed an algorithm to estimate the *3-D* coordinates of a human in real-time using a single camera setup.
- **Project Manas (AI Robotics)** *Feb 2018 - Feb 2019*
  - Worked on clustering and tracking LiDAR point clouds and sensor fusion using Kalman filters for localization in autonomous vehicles.

SELECTED PUBLICATIONS

- **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
- **PROV-FL: Privacy-preserving Round Optimal Verifiable Federated Learning**
  15th ACM Workshop on Artificial Intelligence and Security, 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
- **[Re] GANSpace: Discovering Interpretable GAN Controls**
  ReScience C, 2022
  Vishnu Asutosh Dasu, Midhush Manohar T.K.
- **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
- **POSTER: Another Look at Boyar-Peralta's Algorithm**
  19th International Conference on Applied Cryptography and Network Security (ACNS), 2021
  Anubhab Baksi, Banashri Karmakar, **Vishnu Asutosh Dasu**
- **POSTER: Optimizing Device Implementation of Linear Layers with Automated Tools**
  19th International Conference on Applied Cryptography and Network Security (ACNS), 2021
  Anubhab Baksi, Banashri Karmakar, **Vishnu Asutosh Dasu**
- **Further Insights On Implementation Of The Linear Layer**
  Security and Implementation of Lightweight Cryptography Workshop (SILC), Eurocrypt 2021
  Anubhab Baksi, Banashri Karmakar, **Vishnu Asutosh Dasu**, Dhiman Saha, Anupam Chattopadhyay
- **Following-up on machine learning assisted differential distinguishers**
  Security and Implementation of Lightweight Cryptography Workshop (SILC), Eurocrypt 2021
  Anubhab Baksi, Jakub Breier, **Vishnu Asutosh Dasu**, Xiaoyang Dong, Chen Yi
- **Machine Learning Attacks on SPECK**
  Security and Implementation of Lightweight Cryptography Workshop (SILC), Eurocrypt 2021
  Anubhab Baksi, Jakub Breier, **Vishnu Asutosh Dasu**, Xiaolu Hou
- **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

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

- **Reviewer**, ReScience *August 2022 - Present*

AWARDS AND ACHIEVEMENTS

- **TCS Citation Award** *(3× recipient)*: Received the TCS Citation Award and appreciation from the Chief Technical Officer and Head of TCS Research thrice for outstanding contribution to the organization.
- **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.*