

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
– Supervised by Professor Gary Tan. CGPA: 3.95/4
- **Manipal Institute of Technology (MIT), Manipal** *July 2016 - July 2020*
Bachelor of Technology, Computer Science and Engineering
– Minor in Big Data. CGPA: 8.71/10

ACADEMIC AND WORK EXPERIENCE

- **The Pennsylvania State University** *May 2023 - July 2023*
Graduate Research Assistant *University Park, PA, USA*
– Working on mitigating unfairness and identifying performance bugs in deep learning models.
– *Technologies used:* Python, PyTorch, Numpy
- **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 data.
– *Technologies used:* Python, PyTorch, Huggingface, NLTK, Spacy, Numpy
- **The Pennsylvania State University** *Aug 2022 - Dec 2022*
Graduate Teaching Assistant *University Park, PA, USA*
– Graduate Teaching Assistant for *CMPSC 465: Data Structures and Algorithms, Fall 2022*.
– Responsible for conducting recitations, holding office hours, designing rubrics, and grading assignments.
- **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 novel 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 federated learning framework with differential privacy guarantees.
– *Technologies used:* C/C++, Python, GMP, OpenSSL, PyTorch, Tensorflow, Eigen
- **Citrix R&D** *Jan 2020 - June 2020*
Software Engineer Intern, Citrix Analytics for Security (CAS) *Bangalore, India*
– Developed a trust service to validate API calls, interactive dashboards for data visualization, and optimized GraphQL queries made from the frontend to enable caching and reduce latency.
– *Technologies used:* Java, Javascript, Spring, React.js, GraphQL, Node.js, Jenkins
- **Nanyang Technological University (NTU)** *Dec 2019*
Research Intern *Singapore*
– Developed algorithms and tools to generate optimized ASIC implementations of block ciphers.
– *Technologies used:* Gurobi, SageMath, C/C++, Python
- **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.
– *Technologies used:* Python, PyTorch, Tensorflow, Numpy, OpenCV
- **Tiny Banyan Technologies** *Feb 2019 - May 2019*
Machine Learning Intern *Remote*
– Developed deep learning models to detect humans and firearms from CCTV footage.
– *Technologies used:* Python, Tensorflow, Numpy, OpenCV

- **Indian Statistical Institute** *May 2018 - July 2018*
Kolkata, India
Summer Scholar
 - Attended a summer school on image processing and computer vision. Developed a method to estimate 3-D coordinates of a human from a live video feed using a single camera.
 - *Technologies used:* C++, OpenCV, Eigen
- **Project Manas (AI Robotics)** *Feb 2018 - Feb 2019*
Manipal, India
AI Member, Perception Division
 - Predominantly worked on clustering and tracking LiDAR point clouds and sensor fusion.
 - *Technologies used:* C/C++, Python, ROS, PCL, OpenCV, CUDA, PyTorch, Tensorflow, Numpy

SELECTED PUBLICATIONS

- **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, Natural Language Processing
- **Intermediate:** C++, Java, Javascript, HTML, Cryptography, SQL, Web Development, Computer Vision, Image Processing, Robotics, ROS, Git, Linux
- **Advanced:** Machine Learning, Deep Learning, Trustworthy ML, Python, C, L^AT_EX, Security, Privacy

SERVICE

- **Reviewer**, ReScience

August 2022 - Present

AWARDS AND ACHIEVEMENTS

- **TCS Citation Award** ($3 \times$ 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 2nd in the Interoperability Profiles Challenge and 9th 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*.