Vishnu Asutosh Dasu

(+582) 203-9641 | vdasu@psu.edu | vdasu.github.io | vdasu | vdasu | Vishnu Dasu

Education

Pennsylvania State University — *State College, U.S.A.*

M.S. in Computer Science and Engineering — *Aug. 2022 - May. 2024*

- GPA: 3.95/4.0

Manipal Institute of Technology — *Manipal, India*

B.Tech in Computer Science and Engineering — *Jul. 2016 - May. 2020*

- GPA: 8.71/10.0

Skills

Languages	Python, Java, JavaScript, C, C++
Frameworks	Django, Spring, NodeJS, ReactJS, PyTorch, Tensorflow
Tools	Docker, Git
Databases	MongoDB, MySQL

Work Experience

Pennsylvania State University | Research Assistant — *State College, U.S.A.*

- Worked on mitigating unfairness in deep learning and developing language models for conversational task assistants. *Jan 2023 - Aug. 2023*
- Designed a novel algorithm for processing conversational data and implemented multi-GPU training of LLMs.
- Developed a prototype algorithm that repairs neurons to improve fairness while maintaining model performance.

Tata Consultancy Services | Security Researcher — *Bangalore, India*

- Developed a single-round secure aggregation protocol for federated learning with strong privacy guarantees. *Sep. 2020 - Jun. 2022*
- Enabled users to join or leave the protocol at any time, achieving fully dynamic participation.
- Resulted in a protocol that was 3x faster than related works and published research paper on the topic.

Citrix R&D | Software Engineer Intern — *Bangalore, India*

- Worked as a full-stack developer in the Citrix Analytics for Security (CAS) team. *Jan. 2020 - Jun. 2020*
- 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.

Tata Consultancy Services | Security Research Intern — *Hyderabad, India*

- Worked as a cybersecurity researcher focusing on preventing adversarial attacks on neural networks. *May 2019 - July 2019*
- Developed an algorithm utilizing denoising autoencoders to remove adversarial noise from CNNs.
- Achieved an 86% effectiveness in removing adversarial noise added to ResNet-based CNN models.

Projects

Suspicious IP Detection | Machine Learning for Security

- Designed a novel framework using autoencoders to detect suspicious IPs in an enterprise to mitigate insider threats.
- Designed a data-processing algorithm to feed logs from network monitoring tools into ML models to improve detection.

Side Channel Attacks | Hardware Security

- Helped design a framework to perform side-channel on stream ciphers using ML, MILP, and SMT methods.
- Designed and implemented a novel ML algorithm to identify the hamming weight from oscilloscope hardware traces.

CurrenSee | Android Application

- Developed an Android application to count the value of Indian bank notes from live images using machine learning.
- Designed a simple GUI to assist the visually impaired in using the application.

Theia.ai | iOS Application

- Developed an iOS application to aid the visually impaired traverse unfamiliar external environments.
- Designed an algorithm using CNNs for path planning and traversal using the camera feed.

Accomplishments

2021 **Award**, Received $500 award from DAGsHub for completing the ML Reproducibility Challenge 2021

2020 **Award**, Three-time recipient of TCS Citation Award for outstanding research and contribution to TCS

2019 **Winner**, Best Project Award (Indian Statistical Institute, Kolkata) - 3D coordinate estimation from 2D images

2018 **Runner up**, Intelligent Ground Vehicle Competition (IGVC) - Interoperability Profiles Challenge