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
- Thesis: Mitigating unfairness in deep learning models

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, OpenCV, Numpy, Huggingface
Tools	Docker, Git, Jenkins
Databases	MongoDB, MySQL, Redis

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 prototype algorithms that repairs neurons to improve fairness without compromising model performance.

Tata Consultancy Services | SECURITY RESEARCHER   *Bangalore, India*
- Designed and implemented a federated learning algorithm using homomorphic encryption and differential privacy.   *Sep. 2020 - Jun. 2022*
- Developed a single-round secure aggregation protocol for federated-learning that is 3x faster than related works.
- Designed a data processing algorithm to process network logs for machine learning applications.
- Designed an algorithm using autoencoders to detect malicious behavior from network logs.

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.

Nanyang Technological University | SECURITY RESEARCHER INTERN   *Singapore*
- Developed algorithms to generated optimized hardware implementations of block ciphers.   *Dec. 2019 - Jan. 2020*
- Proposed algorithm generated the best-known implementation of the *AES MixColumn* matrix using XOR2 and XOR3 gates.

Tata Consultancy Services | SECURITY RESEARCHER INTERN   *Hyderabad, India*
- Worked on preventing adversarial attacks on CNNs and explainable AI to understand how CNNs classify images.   *May 2019 - July 2019*
- Developed an algorithm using denoising autoencoders to remove adversarial noise added to RGB images.
- Proposed algorithm was 80% effective in removing adversarial noise added to ResNet-based CNNs.

Projects

Data Extraction from Large Language Models | PRIVACY OF MACHINE LEARNING
- Helped design attacks to extract training data from LLMs trained using federated learning.
- Proposed attack extracts training sequences verbatim from targeted victim participants in federated learning.

Side Channel Attacks on Stream Ciphers | HARDWARE SECURITY
- Helped design a framework to perform side-channel attacks 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 MACHINE LEARNING APPLICATION
- Developed an Android application to count the value of Indian bank notes from live images using machine learning.
- Designed a simple GUI with accessibility features to assist the visually impaired in using the application.

Theia.ai | iOS MACHINE LEARNING APPLICATION
- Developed an iOS application to aid the visually impaired traverse unfamiliar external environments.
- Designed an algorithm using CNNs running on the iPhone for path planning and traversal using the live 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 Research
2019	**Winner,**	Best Project Award out of 13 teams (Indian Statistical Institute, Kolkata) - 3D coordinate estimation from 2D images
2018	**Runner up,**	Intelligent Ground Vehicle Competition (IGVC) - Interoperability Profiles Challenge out of 26 teams