

# Sindhuja Madabushi

Ph.D. Student, Virginia Tech, Blacksburg, VA, USA

✉ msindhuja@vt.edu

☎ (505) 457-7721

➕ <https://sindhujamadabushi.github.io>

## SKILLS

---

Programming & Databases: Python, C#, Java, SQL, JavaScript, Neo4j, MySQL

ML & Data: PyTorch, TensorFlow, NumPy, Pandas, Matplotlib, Librosa, DiffPrivLib, PyTorch Geometric, NetworkX

Tools: Linux, Git, MPI, HPC Slurm, Jupyter

Cloud & MLOps Tools: AWS, GCP, containerization (Docker, Kubernetes)

Web & Visualization: HTML5/CSS3, Bootstrap, d3.js, SharePoint

Explainability: LIME, SHAP, Integrated Gradients, GRAD-CAM, LRP

## RESEARCH EXPERIENCE

---

### Applied ML Researcher (Graduate Research Assistant)

Virginia Tech, Department of Computer Science

Aug 2023 - Present

*Model Reliability, Uncertainty & Failure Analysis:* Surveyed **instance-level failure modes in ML systems**, including misclassification under distribution shift, miscalibration, and long-tailed data.

*Causal Reasoning for Robust ML:* Used intervention-based analysis to separate spurious from disease-relevant signals and study representation effects on explainability in audio-based animal disease detection.

*ML Systems:* Led two projects on scalable distributed trading with differential privacy; **improved client incentives (+25%)**, cut training time, and reduced compute cost while maintaining accuracy.

*ML Explainability & XAI Metrics:* Designed domain-grounded explainability metrics mitigating spurious correlations using consensus models and False Discovery Rate; integrated explanation-aware regularization into training, **improving explanation fidelity by ~15%**.

*Knowledge of Full ML Lifecycle:* Implemented data curation, training, deployment, monitoring for multiple data modalities such as image, audio, video, and tabular. Possess deep understanding of ML optimization techniques.

*Adversarial AI:* Reproduced and extended [label/feature](#) inference and [backdoor](#) attacks, **matching reported accuracy within  $\pm 5\%$**  with tunable severity and client configurations across datasets.

*Audio ML, XAI & Diffusion:* Built an end-to-end audio ML pipeline with diffusion-based listenable explanation synthesis, **cutting labeling noise by ~30%**.

*AI Fairness:* Benchmarked privacy-fairness trade-offs in federated settings, designing loss disparity monitoring that **improved worst-client accuracy by ~25%**.

*Privacy Defenses:* Designed and evaluated defense mechanisms applied **during inference** in federated learning, integrating noise-based strategies **improving privacy by 30x while sustaining high model utility**.

*Benchmarking:* Conducted **benchmarking** and statistical evaluation of machine learning models on audio datasets, including **feature extraction** from spectrograms and hypothesis testing to analyze model performance and reliability.

### Research Associate

University of Wisconsin-Madison, Department of Electrical & Computer Engineering

Jan 2020 - Dec 2022

Led design of a scalable two-cloud algorithm for privacy-preserving DNA read alignment, leveraging advanced data structures and algorithms to process whole-genome, large-scale sequencing (NGS) data. Delivered chromosome-level alignment in minutes with 100% privacy and zero accuracy loss in a privacy-critical medical workload.

## EDUCATION

---

### PhD Candidate

Computer Science  
Virginia Tech (Aug 2023-Present)

### Master of Science

Data and Knowledge Engineering  
OVGU Magdeburg (2016 - 2019)

### Bachelor of Technology

Computer Science  
GITAM University (2009 - 2013)

## INDUSTRY EXPERIENCE

---

### Student Research Intern

PiSA sales GmbH  
2017 - 2018

### Software Engineer 1

Innominds Software  
2015 - 2016

### Systems Engineer

Tata Consultancy Services  
2013 - 2015

## PUBLICATIONS

---

AGRI-Fidelity: Evaluating the Reliability of Listenable Explanations for Poultry Disease Detection

**Sindhuja Madabushi**, Arda Dogan, Jonathan Liu, Dian Chen, Dong S Ha, Sam Noh, Sook Shin, Jin-Hee Cho (Submitted)

MURIM: Multidimensional Reputation-based Incentive Mechanism for Federated Learning

**Sindhuja Madabushi**, Dawood Wasif, Jin-Hee Cho (ArXiv 2025) [\[PDF\]](#)

PRIVEE: Privacy-Preserving Vertical Federated Learning Against Feature Inference Attacks

**Sindhuja Madabushi**, Haider Ali, Ahmad Faraz Khan, Ananthram Swami, Rui Ning, Jin-Hee Cho (ArXiv 2025) [\[PDF\]](#)

OPUS-VFL: Incentivizing Optimal Privacy-Utility Tradeoffs in Vertical Federated Learning

**Sindhuja Madabushi**, Ahmad Faraz Khan, Haider Ali, Jin-Hee Cho (ArXiv 2025) [\[PDF\]](#) [\[CODE\]](#)

Empirical Analysis of Privacy-Fairness-Accuracy Trade-offs in Federated Learning: A Step Towards Responsible AI

Dawood Wasif, Dian Chen, **Sindhuja Madabushi**, Nithin Alluru, Terrence J Moore, Jin-Hee Cho (AIES 2025) [\[PDF\]](#)

Two-Cloud Private Read Alignment to a Public Reference Genome

**Sindhuja Madabushi**, Parameswaran Ramanathan (PETS 2023) [\[PDF\]](#) [\[CODE\]](#)

## AWARDS AND HONORS

---

**Cyber Innovation Scholar program: Commonwealth Cyber Initiative (CCI), Southwest Virginia (SWVA) Node**

Awarded \$1,500 for professional development, startup development, and entrepreneurship training.

**Elected Secretary:** Computer Science Graduate Council, Virginia Tech, 2025-2026

Chosen by peers to represent the graduate student body, coordinate initiatives, and advocate for student interests.

**Best Poster Award:** Commonwealth Cyber Initiative Southwest Virginia Student Researcher Showcase, 2025

Recognized for excellence in presenting original research in privacy-preserving Federated Learning.

**Travel Awards:** ACM Capital Region Celebration of Women in Computing (CAPWIC) 2024 & 2025; Conferencship Travel Award, Annual Computer Security Applications Conference (ACSAC) 2023.

## SERVICE

---

**Research Mentor:** Mentored 2 undergraduate students at VT (Arda Dogan and Jonathan Liu) as part of NSF Research Experiences for Undergraduates (REU) program during Fall 2025 to present.

**Peer Reviews:** IEEE Transactions on Network and Service Management (3 review), IEEE Transactions on Services Computing (2 reviews), IEEE Transactions on BigData (1 review).

**Volunteer, Computers and Technology at VT (C-Tech<sup>2</sup>) Program:** Virginia Tech, Summer 2025, delivered outreach workshops for high school students, introducing optimization concepts and problem-solving activities.

**Volunteer, STEM Santa Fe:** Nonprofit organization that delivers STEM programs, mentoring, and resources, 2022  
Led a mentoring team for ~100 school students, inspiring participants to explore STEM careers.

**Master's Mentor:** Otto-von-Guericke University, 2017-2018: Organized orientation events and provided mentorship to over 100 incoming international graduate students, **Organizer:** Magdeburg Indians NGO, 2017-2018: Directed the cultural team for community events, including a summer festival with ~1,000 attendees.