SUDHARSHAN BALAJI

Email : sudharshanbalaji@usf.edu
https://sudharshanbalaji.com
Mobile : +1 (656) 216-5583
GitHub: https://github.com/bsudharshan2001
LinkedIn: https://www.linkedin.com/in/sudharshanbalaji

Education

Doctor of Philosophy, Computer Science May 2030
University of South Florida, Tampa, FL

Master of Science (Thesis Track), Computer Science May 2025
University of South Florida, Tampa, FL

Bachelor of Engineering, Computer Science and Engineering June 2023
Amrita University, Coimbatore, India

Relevant Courses: Machine Learning, Neural Networks and Deep Learning, Security & Privacy in ML, Software Engineering, Mining of Massive Datasets, Fundamentals of Data Science, Topics in NLP, Introduction to AI, Privacy Preserving Trustworthy-Cyberinfrastructures

Skills

Programming Languages:	Python, C, C++, Java, Dart
Database Management:	MySQL, MongoDB
Productivity Tools:	Microsoft Office 365, Jira, Git
AI & ML Domains:	Computer Vision, Recommender Systems, LLMs, Federated Learning
Frameworks & Libraries:	PyTorch, TensorFlow, Keras, OpenCV, HuggingFace Transformers, Flask
Web Development:	HTML, CSS, JavaScript, NodeJS

Experience

Graduate Research Assistant - SPRAI Lab, USF, Tampa, FL, USA Aug 2025 - Present

- Continuing doctoral research under Prof. Ning Wang focused on Byzantine-resilient Federated Learning and the security aspects of large language models (LLMs).
- Conducting multi-wave experiments using Flower-based federated learning testbeds with Raspberry Pi and Jetson devices, investigating effects of model poisoning on non-IID data distributions and Byzantine aggregation robustness.

Graduate Instructional Assistant - SPRAI Lab, USF, Tampa, FL, USA Sep 2024 - May 2025

- Conducted thesis research on security applications of large language models titled "LLMs for Network Intrusion Detection: A Comprehensive Analysis" working with Graduate Advisor Prof. Ning Wang to comprehensively analyze methodologies and exploring the use of LLMs, MLMs, and MLM embeddings for network intrusion detection across scales (Successfully defended the thesis - Link to thesis).
- Built coursework, supporting instruction and grading for two courses, "Privacy Preserving Trustworthy Cyber-Infrastructures" under Prof. Attila Yavuz, and "Human Aspects of Cybersecurity" under Graduate Advisor Prof. Ning Wang, during Spring 2025.
- Supported instruction and grading for "Security and Privacy in ML" under Prof. Guangjing Wang, assisting students with questions during office hours and helping ensure clarity in assessments for a class of $\sim$ 100 in Fall 2024.

Machine Learning Engineering Intern - dotkonnekt Innovation Labs, Bangalore March 2023 - July 2023

- Contributed to a cross-functional team of engineers, scientists, and product managers to successfully develop and deploy machine learning models and algorithms for the company's D2C Experiential Platform, enabling personalized shopping experiences
- Implemented a cutting-edge recommender engine, encompassing content-based filtering systems, collaborative filtering systems, and hybrid recommenders, for the company's D2C platform
- Integrated Huggingface models with LangChain, including open-source language models such as BERT and Falcon-40B, into the company's platform, contributing significantly to the platform's language processing capabilities
- Leveraged AWS SageMaker for model training, proficiently experimenting with various instance types to optimize model performance
- Deployed models using Node.js and Flask, ensuring seamless integration with existing infrastructure and an improved user experience.

Projects

Development of CADRADs Prediction System: Jun 2024 - Present

- Spearheaded the development of CCTA-RADS, the largest publicly available dataset of 940 real-world Coronary CT Angiography (CCTA) reports from Tampa General Hospital, annotated with expert-verified CAD-RADS scores under IRB approval.
- Lead a multi-disciplinary collaboration with Prof. Ning Wang (USF SPRAI Lab), Dr. Zhiyu Liu, Dr. Shone Almeida, and Dr. Mathew Karvelil (USF Morsani College of Medicine) to address linguistic and structural heterogeneity in clinical text
- Designed an end-to-end two-stage Clinical NLP pipeline for automated CAD-RADS scoring, integrating an LLM-based report parser (ChatGPT-4o-mini, Mistral DocAI, GPT-4.1) that normalizes free-text reports with fine-tuned BERT-family classifiers (BioBERT, ClinicalBERT) trained on structured JSON data
- Achieved a 90.12% F1-score with BioBERT, surpassing direct LLM prompting and raw-text fine-tuning methods, while improving classification of clinically critical CAD-RADS classes (3-4) and non-diagnostic cases (N).
- Developed a HIPAA-compliant text-processing and data sanitization pipeline to ensure secure report handling and consistent terminology standardization across all training stages.
- Integrated explainable AI (SHAP, LIME) for model interpretability, enabling visualization of key sections influencing each prediction to enhance clinical transparency and trust.
- Deployed the trained model as a web-based clinical decision-support tool, allowing radiologists to upload de-identified reports for automated scoring with interpretability visualizations
- Funded by USF Morsani College of Medicine through Graduate Medical Education Fund: $5000
- *Publishing research as a paper - "Learning from Textual Radiology Reports: A Benchmark Dataset for Coronary CT Angiography" - Under review at EACL 2025*

Crowd Counting Using Wi-Fi CSI: May 2022 - Jun 2023

- Developed an innovative solution for crowd estimation utilizing Wi-Fi Channel State Information (CSI), aiming to overcome limitations in accuracy, scalability, cost and privacy encroachment in traditional methods.
- Deployed ESP32 microcontrollers to design and execute controlled experiments, collecting custom CSI datasets across varying room configurations (8ft x 8ft and 10ft x 10ft) and occupancy levels (1-6 people) to address data scarcity challenges
- Applied advanced data augmentation techniques to account for environmental variability in CSI data, exploring calibration and synthetic enrichment strategies to improve training dataset robustness
- Implemented and trained neural networks using TensorFlow, Keras and Scikit-learn to process and analyze Wi-Fi CSI data

Development of Generic Mitigation systems against ransomware: Apr 2022 - Dec 2022

- Project funded by the Department of Science and Technology, Government of India under Science and Engineering Research Board (SERB).
- Developed a robust analysis test-bed to effectively monitor the run-time behavior of ransomware
- Created a standardized ransomware dataset alongside ransomware behavior model to develop a generic ransomware mitigation system.

Varuna - Cyclone Intensity Estimation Dashboard: Feb 2022 - Mar 2022

- Designed and developed a Tropical Cyclone Intensity Estimation web application using CNN-based architectures (R-CNN, Faster R-CNN, YOLO) in Flutter, leveraging half-hourly INSAT-3D IR satellite imagery
- Implemented an automated data-fetching pipeline to regularly retrieve images from the IMD website (in the absence of an API) for real-time model inference. Built and presented as part of the Smart India Hackathon (SIH 2022) organized by the Government of India.

Civitas - Community Management App: Sep 2021 - Oct 2021

- Designed and built a cross-platform app that can assist general community service requirements like booking complaints, garbage collection, parking manager and neighbor connect along with added chat-bot features to assist in natural query helping for HoneyWell Smart City Hackathon 2021.
- The app was built using Flutter, Dialogflow, Weather and News API.

Achievements & Scholarships

- Lead a team to Design and Develop a Community Management App using Flutter for HoneyWell Smart City Hackathon 2021. Placed among Top 25 Teams all over India.
- Amrita Vidhyanidhi Scholarship: Awarded 90% of the tuition fee waiver for the entirety of bachelor's degree