

# Sri Hrushikesh Varma Bhupathiraju

Email: [bhupathirajus@ufl.edu](mailto:bhupathirajus@ufl.edu) | [Google Scholar](#) | [Personal Portfolio](#)

## EDUCATION

---

**PhD in Computer Information Science and Engineering** | University of Florida **Dec 2025**  
Research Area: Cyber-Physical Systems Security.  
Advisor: Prof. Sara Rampazzi

**Master of Science in Computer Information Science and Engineering** | University of Florida **May 2021**  
Research Area: Medical Image Analysis  
Advisor: Prof. Sanjiv Samant

**Bachelor of Technology in Electronics and Communications Engineering** | JNTU University **May 2019**  
Research Area: Signal and Image Processing  
Advisor: Prof. Sanjay Dubey

## RESEARCH INTERESTS

---

My research focus is on the security of cyber-physical systems security, with emphasis on enhancing the security of perception sensors and the subsequent signal processing and machine learning algorithms used in safety-critical systems such as autonomous vehicles. To this end, my research focuses on uncovering new vulnerabilities and potential risks in critical parts of autonomous driving systems, such as perception, prediction, and planning. My research also includes investigating countermeasures against these vulnerabilities using physical invariability in sensor characteristics, contextual information, and machine learning techniques. Using my research, I aim to contribute to more robust cyber-physical and autonomous systems, ensuring the safety of the people who use them and increasing their trust in these technologies.

## PROFESSIONAL EXPERIENCE

---

**Cyber-Physical Systems Security (CPSec) Lab, University of Florida** **Jan 2021 – Present**

- Discovered and analyzed vulnerabilities in perception sensors, autonomous system signal processing pipelines and their implications on downstream tasks.
- Studied and evaluated new physical world vulnerabilities in traffic sign and traffic light recognition systems used in autonomous vehicles.
- Designed novel defense strategies based on the invariable physical properties of the sensor that detect and mitigate the attack in an autonomous vehicle setting

**Davis Cancer Research Center, Radiation Oncology, UF Health** **Dec 2020 - Aug 2021**

- Implemented dimensionality reduction algorithms to compute the displacement fields, used to deform CT images and track organ motion.
- Worked on the Triangulation method to track the deformed GTV surface and on a Deep texture classification model.
- Designed LSTM-based deep learning models to predict organ-specific abdominal motion with Cine-MRI.

**Modern Artificial Intelligence and Learning Technologies Lab, University of Florida** **May 2020 - Aug 2020**

- Worked on a project that involved building intelligent algorithms for transportation and smart cities.
- Implemented an algorithm that predicts the traffic patterns across intersections using real-time data received from LiDAR sensors.
- Constructed the residual data across intersections, performed clustering, and classified them into events.

### Teaching Assistant

Cyber-Physical System Security, Graduate Teaching Assistant, CISE Dept., UF. **Fall 2022**  
Supervisor: Dr. Sara Rampazzi.

- Assisted a class of 90 students in a course on Cyber-Physical Systems and Security.
- Provided lectures on physical adversarial example modeling and training. Assisted students in simulating physical adversaries and testing as part of the lecture.

Digital Image Processing, Undergraduate Teaching Assistant, ECE Dept., BVRIT, JNTU. **Spring 2019**  
Supervisor: Dr. Syed Audhagir Umar.

- Instructed a class of 60 students, covering fundamental concepts such as denoising and image reconstruction.
- Guided hand-on projects helping students build real-world techniques such as image in-painting and object detection.

## PUBLICATIONS

---

- **[NDSS '24]** Takami Sato\*, **Sri Hrushikesh Varma Bhupathiraju\***, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, and Sara Rampazzi, "Invisible Reflections: Leveraging Infrared Laser Reflections to Target Traffic Sign Perception." (\* denotes co-first).
- **[IEEE S&P '24]** Jennifer Sheldon, Weidong Zhu, Adnan Abdullah, **Sri Hrushikesh Varma Bhupathiraju**, Takeshi Sugawara, Kevin R. B. Butler, Md Jahidul Islam, and Sara Rampazzi. "AquaSonic: Acoustic Manipulation of Underwater Data Center Operations and Resource Management."
- **[VehicleSec '24]** **Sri Hrushikesh Varma Bhupathiraju**, Takami Sato, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, and Sara Rampazzi. "Short: On the Vulnerability of Traffic Light Recognition Systems to Laser Illumination Attacks."
- **[Phys. Med. Biol. '24]** Jingxi Weng, **Sri Hrushikesh Varma Bhupathiraju**, Thomas Samant, Alex Dresner, Jian Wu, Sanjiv S Samant. "Convolutional LSTM model for cine image prediction of abdominal motion."
- **[ACM WiSec '23]** **Sri Hrushikesh Varma Bhupathiraju**, Jennifer Sheldon, Luke A. Bauer, Vincent Bindschaedler, Takeshi Sugawara, and Sara Rampazzi. "EMI-LiDAR: Uncovering Vulnerabilities of LiDAR Sensors in Autonomous Driving Setting Using Electromagnetic Interference."
- **[VehicleSec '23]** Takami Sato\*, **Sri Hrushikesh Varma Bhupathiraju\***, Michael Clifford, Takeshi Sugawara, Qi Alfred Chen, and Sara Rampazzi. "WIP: Infrared Laser Reflection Attack Against Traffic Sign Recognition Systems." (\* denotes co-first), (**Best Paper Award**).
- **[USENIX '23]** Yulong Cao, **Sri Hrushikesh Varma Bhupathiraju**, Pirouz Naghavi, Takeshi Sugawara, Z. Morley Mao and Sara Rampazzi. "You Can't See Me: Physical Removal Attacks on LiDAR-based Autonomous Vehicles Driving Frameworks."
- **[AAPM '23]** Jingxi Weng, Mohammad Anas, **Sri Hrushikesh Varma Bhupathiraju**, Thomas Samant, Alex Dresner, Jian Wu, Sanjiv S Samant. "Organ-Specific Abdominal Motion Prediction Using Deep Learning with Cine-MRI."

## SELECTED PROJECTS

---

### Leveraging Infrared Laser Reflections to Target Traffic Sign Perception

- Develop an effective physical-world attack that leverages the sensitivity of filterless image sensors and the properties of Infrared Laser Reflections (ILRs), which are invisible to humans.
- Designed attack to undermine the traffic sign recognition by inducing misclassification and formulated the threat model and requirements for an ILR-based traffic sign perception attack to succeed.
- Evaluated the effectiveness of the attack in real-world driving scenarios and designed detection techniques based on physical properties of laser reflections
- Paper presented at NDSS 2024. Project Website: [Invisible Reflections](#)

### Vulnerabilities of LiDAR Sensors to Electromagnetic Interference

- Exposed a new threat in the form of Intentional Electro-Magnetic-Interference (IEMI), which affects the time-of-flight (TOF) circuits that make up modern LiDARs.
- Demonstrated that these vulnerabilities can be exploited to force the AV Perception system to misdetect, misclassify objects, and perceive non-existent obstacles.
- Proposed countermeasures that detect the attack by analyzing the geometric constraints of the LiDAR point cloud
- Paper presented at ACM WiSec 2023. Project Website: [EMI LiDAR](#)

### Attack on LiDAR-based Autonomous Vehicles Driving Frameworks

- Studied the reliability of medical devices from a security and safety perspective.
- Demonstrate that adversaries could remotely manipulate critical health devices using various types of signal injection.
- Proposed countermeasures that detect the attack based inconsistency in LiDAR sensor data.
- Paper presented at USENIX 2023. Project Website: [You Can't See Me](#)

## ACHIEVEMENTS

---

- CSAW Applied Research Competition finalist, 2024 (Top 7.5%).
- ETAS Best Short Paper Award, VehicleSec '23.
- DENSO Best Demo Award, VehicleSec '23.
- Student Travel Grant Award, USENIX '23.
- Student Travel Grant Award, ACM WiSec '23.

- Student Travel Grant Award, VehicleSec '23, '24.

## **ACADEMIC SERVICES**

---

- Student volunteer, Symposium on Vehicle Security and Privacy (VehicleSec) 2023, 2024.
- PC committee, poster and demo session, VehicleSec 2024.
- More than 5 papers review experience as a delegation reviewer (USENIX, IEEE S&P)