SAI THARUN REDDY MULKA

Ph.D. Student | S3 Lab | University of Texas at Dallas

Email | Github | Linkedin| Scholar

S3 Lab | Robotics Security | CPS Fuzzing

RESEARCH INTERESTS: Hardware-Assisted Security | Agentic Safety in Robotics | LLM+RL Guided CPS Fuzzing | Secure Autonomy and Control Systems

SUMMARY

Ph.D. researcher in the **Software & Systems Security (S3 Lab)** at the **University of Texas at Dallas**, advised by **Dr. Chung Hwan Kim**. My research broadly focuses on **systems and hardware security**, with applications in **cyber-physical systems**, **robotics**, and **trustworthy AI**. I aim to design **trustworthy and resilient computing foundations** that allow intelligent systems to interact safely with complex physical environments. Supported by agencies including the **NSF**, **Agency for Defense Development**, and the **U.S. Department of Transportation**. Actively seeking **Security Research** or **Security Engineering** internships focusing on **systems security**, **CPS/robotics protection**, and **AI safety**.

EDUCATION

University of Texas at Dallas – **Ph.D., Computer Science (Security)** *Aug 2023 – May 2028 (expected)*

- Advised by **Dr. Chung Hwan Kim**, Software and Systems Security **(S3 Lab)**
- Research on security for robotics and cyber-physical systems, focusing on physical-layer device authentication, agentic AI safety, and coverage-driven fuzzing for autonomous control loops.

University of Texas at Dallas – **M.S., Computer Science (Security)** *Aug 2023 – May 2025*

- Coursework: Advanced Operating Systems, Systems Security and Binary Code Analysis, Machine Learning.
- Awards: ***Jonsson School Dean's Graduate Scholarship (2023 - 2024)***

Vellore Institute of Technology – B.Tech., Computer Science (Networking & Security) *Jun 2019 – Jun 2023*

- Thesis: *A Comprehensive Examination of Email Spoofing*; Advisor: **Dr. Sibi Chakkaravarthy Sethuraman**
- Awards: ***Dean's Research Excellence Award (2020)***

RESEARCH EXPERIENCE

Research Assistant

Spring 2024 – Present

Software & Systems Security (S3 Lab), University of Texas at Dallas

VOLTRON: Physical-Layer Authentication for USB Peripherals Spring 2024 – Fall 2025

Key Technologies: Python, Machine Learning, Signal Processing, Hardware Security, USB Protocol Analysis

- Designed a **zero-trust USB peripheral authentication system** that verifies device identity from **electrical-layer signal characteristics** with **no hardware, firmware, or OS modifications**.
- Engineered a **feature extraction pipeline** combining **transient response analysis**, **frequency-domain spectral signatures (FFT)**, and **envelope-based statistical descriptors** to capture **device-intrinsic physical fingerprints**.
- Developed a **robust adversarial threat model** covering impersonation attacks, cable/port variation, voltage noise, and session drift; validated identity stability across **70+ commercial USB devices**.
- Achieved **high identification accuracy** under environmental changes with **negligible runtime overhead**, demonstrating **practical deployability at the hardware interface layer**.

Agentic AI for Autonomous Robotics Control & Safety Fall 2025 – Present

Key Technologies: ROS2, Agentic Frameworks, NVIDIA Isaac Sim, MoveIt2

- Investigating **trustworthiness and safety** of **LLM-driven robotic control systems**, focusing on failure modes in perception grounding, action planning, and actuator-level execution.
- Constructed an **agentic control architecture** where LLMs perform **task reasoning, tool selection, and motion planning** through **ROS2 action and topic interfaces** to a Franka Panda manipulator in **NVIDIA Isaac Sim**.
- Developed a **closed-loop state feedback layer** using **ROS Topics**, and object-pose streams to support **self-correction and adaptive re-planning**.

- Benchmarked LLM-generated motion plans against **MoveIt2 classical planners** to characterize **systematic grounding and frame-alignment errors**, identifying core **robustness gaps**.

Vision–Language–Action (VLA) Framework for Grounded Robotic Manipulation Fall 2025 – Present
Key Technologies: OpenVLA, RT2, PyTorch, ROS2, Hugging Face, NVIDIA Isaac Sim, CUDA

- Constructed a **vision–language–action control pipeline** that fuses **RGB/depth features** (CLIP/ViT) with **LLM reasoning** (OpenVLA/GPT-4V) to produce **robot manipulation actions**.
- Designed an **action decoding layer** that maps natural-language task goals into **joint-space trajectories** and gripper movements via **ROS2** motion control interfaces.
- Implemented **multimodal fusion mechanisms** to strengthen **scene grounding** and reduce **hallucinated or physically infeasible action outputs**.
- Working on mitigating failure cases such as **depth misalignment** and **ambiguous object references** by refining **data sampling**, scene labeling, and prompt-conditioning strategies.

Secure Causally Ordered Broadcast System for Distributed Environments Spring 2024
Key Technologies: Java, TCP/IP Sockets, POSIX Threads, Vector Clocks, Wireshark, Linux

- Extended the classic **Causally Ordered Broadcast** algorithm to integrate **security and fault-tolerance primitives** within a distributed process communication framework.
- Designed a **four-node distributed architecture** using **TCP sockets and multithreading**, ensuring message delivery preserves causal order via **vector-clock synchronization**.
- Incorporated **message authentication and integrity validation** using **SHA-256 hashing** and replay-protection mechanisms to mitigate message spoofing and tampering.
- Conducted stress testing under **randomized network delays and buffer perturbations** (1–5 ms) to evaluate message ordering stability and system robustness.

TEACHING EXPERIENCE

Teaching Assistant
Fall 2023 – Present

Department of Computer Science University of Texas at Dallas

- **Courses:** Computer Networks (Fall 2023), Wireless Networks (Spring 2024), Database Systems (Fall 2024), Computer Networks (Spring 2025), Database Systems (Summer 2025), **Advanced Wireless Networks (Fall 2025)**.
- Guided weekly discussion and lab sessions covering **network protocols**, **wireless communication systems**, and **database design**, supporting both undergraduate and graduate students.
- Provided **technical mentorship** to students on course projects, explaining core concepts such as routing, TCP/UDP behavior, query optimization, and **wireless PHY/MAC interactions**.

PUBLICATIONS

VOLTRON: Physical-Layer Fingerprinting for USB Device Authentication[PDF]. **[USENIX Security, Rebuttal Stage, 2025]**

A Comprehensive Examination of Email Spoofing: Issues and Prospects for Email Security[PDF]. **[Computers & Security, 2023]**

An Artificial Neural Network Autoencoder for Insider Cyber Security Threat Detection[PDF]. **[Future Internet, 2023]**

Artificial Intelligence in Higher Education[PDF]. **[IGI Global, 2022]**

TECHNICAL SKILLS

Security: Cyber-Physical Systems (CPS) Security, Robotics Security, USB/Peripheral Trust, Fuzzing and Adversarial Testing, Threat Modeling, Reverse Engineering, Binary Instrumentation
AI / Machine Learning: PyTorch, TensorFlow, scikit-learn, NLP (NLTK, Transformers), Reinforcement Learning, Anomaly Detection, Adversarial ML
Robotics & Systems: ROS2, Gazebo, DDS Middleware, NVIDIA Isaac Sim, MoveIt2, Linux, Docker, Git, CI/CD Automation, Sensor–Actuator Integration
Programming & Tools: Python, C/C++, Rust, Bash, SQL, Java, JavaScript, HTML/CSS; Wireshark, Scapy, GDB, Valgrind, GitHub Actions