Sihat Afnan

@ sihata@uci.edu | LinkedIn | GitHub | Portfolio | Irvine, CA

Education

University of California, Irvine — Irvine, CA
PhD in Computer Science; ***GPA: 3.97/4.00*** — *Sep 2024 – Present*

Bangladesh University of Engineering and Technology — Dhaka, Bangladesh
B.Sc. in Computer Science and Engineering; ***GPA: 3.81/4.00*** — *April 2018 – Jun 2023*

Graduate Courses at UCI

- Robotics Deep Learning (CS295)
- Computer and Systems Security (CS205)
- Network and Distributed Systems Security (CS203)
- Machine Learning (CS273A)
- Systems and ML (CS256)
- Image Understanding (CS216)
- Embedded and Ubiquitous Systems(CS244)
- Usable Security and Privacy (CS204)
- Computer Networks (CS232)

Skills

Languages: C/C++, C#, Java, Python, Go, SQL, Swift
Frameworks: Unity, Unreal, ARKit, Django, PyTorch, TensorFlow
Hardware: Arduino, Raspberry Pi, ATMega32
Version Control System: Git

Experience

University of California, Irvine — Irvine, CA
Teaching Assistant — *Sept 2024 – Present*

- CS 130: Introduction to Computer Security
- ICS 33: Intermediate Programming with Python
- ICS H32: Python Programming with Libraries (Accelerated)

Brac University — Dhaka, Bangladesh
Lecturer — *June 2023 – Aug 2024*

- CSE341 (Microprocessors)
- CSE340 (Computer Architecture)
- CSE321 (Operating Systems)
- CSE230 (Discrete Mathematics)

Research Experience

Security/Privacy of Robotics

- Showed that human-to-humanoid motion retargeting, which projects operator demonstrations onto a shared robot skeleton and discards body shape, fails to anonymize the operator: while it normalizes body proportions, it preserves movement dynamics shaped by the operator's physiology. Demonstrated that retargeted trajectories support accurate gender classification, operator reidentification, and age/height regression even for unseen operators, with signals that are task-invariant and consistent across retargeting implementations. Introduced UNVEIL, a skeleton-aware spatiotemporal graph network to measure and interpret this effect, raising a privacy

concern for the robotics community: as teleoperation datasets are increasingly shared and scaled, retargeted trajectories can act as a biometric fingerprint exposing sensitive operator attributes.Project Page: https://project-unveil.github.io/

Status: Under review at NEURIPS 2026

Security of AR/VR Systems

- Investigated the security of XR spatial understanding pipelines by designing the first on-device acoustic attack that uses only a headset's built-in speakers to subtly manipulate 3D scene reconstruction. Modeled how injected acoustic interference perturbs camera odometry, RGB imaging, and depth sensing, and developed an optimization framework that generates perturbations causing controlled geometric distortions in the spatial map. Demonstrated impactful effects including object addition/removal, surface misclassification, and degraded user task performance across Meta Quest 3S, Apple iPad, and ARIA glasses, with real-world experiments on Quest 3S showing corruption in over 91% of spatial maps.

  Status: Under review at Mobicom 2026

Autonomous Vehicle Security

- Developing a high-fidelity VR simulation framework using CARLA to study how human drivers perceive and react to autonomous vehicle misbehavior caused by sensor-level perception attacks such as stop sign manipulation, lane detection failures, and phantom obstacles. The project integrates a realistic AV stack, including sensor simulation, machine-learning based perception, planning, and control, together with real-time eye-tracking and behavioral logging. This work addresses key challenges in synchronizing multi-modal sensor data, attack injection, and human–autonomy interaction in VR, enabling systematic evaluation of AV safety under adversarial conditions.

  Status: Under review at IEEE S&P 2027

LLM Based Threat Detection

- A framework designed to detect APT attack patterns leveraging the power of self-attention in transformers. We incorporate customized embedding layers to effectively capture the context of event sequences derived from provenance graphs. While acknowledging the computational overhead associated with training transformer networks, our framework surpasses existing LSTM and Language models regarding APT detection performance. We integrated the model parameters and training procedure from the RoBERTa model and conducted extensive experiments on well-known APT datasets (DARPA OpTC and DARPA TC E3). Our framework achieved superior F1 scores of 98% and 95% on the two datasets respectively, surpassing the F1 scores of 96% and 94% obtained by LSTM models. Our findings suggest that LogShield's performance benefits from larger datasets and demonstrates its potential for generalization across diverse domains.

  Status: ArXiv

Projects

LiDAR Scanner

- Developed sensor scanner application capable of collecting raw LiDAR-based scene data—including 3D depth frames, confidence frames, RGB frames and per-frame camera intrinsic/extrinsic parameters. The application ahs two version, one that runs on Apple Vision Pro, iPad Pro, and other LiDAR-equipped devices, another that runs on Meta Quest XR headsets. It was designed as a research tool for XR perception and spatial computing.

Flow Classification on Data Plane Using P4 Switch

- Implemented early-stage classification of long-lived and short-lived network flows using P4 framework. Trained a decision tree classifier offline and deployed the inference logic directly on P4 switches for real-time operation. Built and evaluated the switch architecture in Mininet using a data center topology to demonstrate accuracy and low-latency inference on the data plane.

Improving RTT & RTO (Peak-Hopper Implementation)

- Developed an open-source implementation of *The Peak-Hopper*, a new retransmission timeout algorithm for reliable unicast transport. Integrated the protocol into the NS-3 network simulator to evaluate improvements over the standard RTO mechanism defined in RFC 2988. Demonstrated gains in responsiveness and throughput under varying congestion and delay conditions.

Smart Stick for the Visually Impaired

- Built an embedded system using an ATMega32 microcontroller with ultrasonic sensing, vibration feedback, and directional guidance to detect obstacles and assist visually impaired users in navigation. Designed custom firmware, sensor fusion logic, and real-time alert mechanisms for safe and efficient mobility support.

Academic Recognition

Computer Science Department Research Fellowship (UCI): Awarded for outstanding research contributions

University Dean's List Scholarship (BUET): Received for academic excellence across Level 1 to Level 4 of undergraduate study.

University Merit List Scholarship (BUET): Awarded for achieving top academic performance in the department.

Talentpool Scholarship (HSC / O Level): Achieved 8th position in Dhaka Board.

Talentpool Scholarship (SSC / A Level): Achieved 20th position in Dhaka Board.