



MAHER AL ISLAM

Graduate Research Assistant, West Virginia University, USA

✉ maherislam071@gmail.com  [mahermayer.github.io](https://github.com/mahermayer)  [maher-al-islam](https://www.linkedin.com/in/maher-al-islam)

RESEARCH INTEREST

- Autonomous Vehicles
- Cybersecurity
- AI Safety & Ethics
- Adversarial AI
- Cyber-Physical System

TECHNICAL SKILLS

- **Artificial Intelligence:** Adversarial AI (FGSM, PGD, UAP, DeepFool); Vision AI (YOLO, UNet, ViT); Context-Aware AI; Reinforcement Learning (Q-Learning, DQN, MDP); Multimodal Sensor Fusion (Camera, LiDAR)
- **Autonomous Systems:** ROS, CARLA, Duckietown; Perception–Control Integration; Control Methods (PID, RL, MPC); CPS Modeling (Smart Homes, Smart Water Distribution)
- **Cybersecurity:** CPS/IoT Security; Game-Theory; Intrusion Detection & Response; Adversarial BSM Detection in CAVs; CTF (Crypto, Cracking, Network, Scanning, Forensics)

EDUCATION

West Virginia University (Advisor: Dr. Amr El-Wakeel)

Ph.D. in Computer Engineering

August, 2024 – Ongoing

WV, USA

Virginia Commonwealth University (Advisor: Dr. Sherif Abdelwahed)

M.S. in Electrical & Computer Engineering GPA: 4.0/4.0

January, 2021 – May, 2024

VA, USA

University of Dhaka

B.Sc. in Electrical & Electronic Engineering GPA: 3.41/4.0

Jan, 2012 – October, 2016

Dhaka, Bangladesh

CURRENT POSITION

iCPS Lab

Graduate Research Assistant

Aug 2024 – Present

Morgantown, WV, USA

- Conducting research in adversarial AI, trustworthy autonomy, and CPS security with applications to autonomous vehicles (AVs) and robotics.
- Developing resilient AI models for real-world deployment in AVs, focusing on perception–control pipelines through context-aware object detection, semantic segmentation, and multimodal sensor fusion.
- Contributing to DARPA's **AI CRAFT (2024–26)** program on resilient AI and cybersecurity for robotics, addressing perception, control, and communication vulnerabilities in CPS.

PEER-REVIEWED PUBLICATIONS [GOOGLE SCHOLAR LINK](#)

[J1] Islam, Maher Al; Srivastava, Anurag K.; El-Wakeel, Amr S., "AI in Autonomous Vehicles Under Siege: Vulnerabilities, Challenges, and Path Forward." Manuscript received in IEEE Transactions on Intelligent Vehicles (In Review).

[C1] M. Al Islam, El-Wakeel, "Towards Context-Aware Autonomous Driving in Degraded Urban Environments using LaneNet." Submitted to IEEE International Conference on Robotics and Automation (ICRA), September 2025. (Submitted)

[C2] **M. Al Islam**, El-Wakeel, **"Integrating Perception and Control for Resilient Autonomous Driving under Vision Adversarial Attacks."** In preparation for IEEE Intelligent Vehicles Symposium, November 2025. (In Progress)

[C3] M. Zaman, **M. Al Islam**, N. Zohrabi and S. Abdelwahed, **"A Machine Learning-Based Temperature Control and Security Protection for Smart Buildings"**, 2024 IEEE International Conference on Smart Computing (SMARTCOMP), Osaka, Japan, 2024

[C4] M. Zaman, **M. A. Islam**, A. Tantawy and S. Abdelwahed, **"An Uncertainty Based Predictive Analysis of Smart Water Distribution System Using Bayesian LSTM Approach"**, 2022 6th International Conference on Universal Village (UV), Boston, MA, USA, 2022

[C5] **M. Al Islam**, C. J. Fung, A. Tantawy and S. Abdelwahed, **"A Game-Theoretic Model for DDoS Mitigation Strategies with Cloud Services"**, NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, Budapest, Hungary, 2022

[C6] Zohrabi, N., Martin, P.J., Kuzlu, M., Linkous, L., Eini, R., Morrissett, A., Zaman, M., Tantawy, A., Gueler, O., **Al Islam, M.** and Puryear, N., 2021, September. **Opencity: An open architecture testbed for smart cities.** 2021 IEEE International Smart Cities Conference (ISC2)

[C7] M. Zaman, **M. Al Islam**, A. Tantawy, C. J. Fung and S. Abdelwahed, **"Adaptive Control for Smart Water Distribution Systems"**, 2021 IEEE International Smart Cities Conference (ISC2), Manchester, UK, 2021

POSTERS & PRESENTATIONS

- **M. Al Islam** et al., WVU AI Symposium (3rd Place), WVU, April 2025
- **M. Al Islam** et al., (Best Poster) **OpenCyberCity Testbed's Recent Progress in Smart City Management**, IEEE SmartComp, June 2024
- **M. Al Islam** et al., **Towards Sustainable Urban Futures: Advancing Urban Tech with the OpenCyberCity Testbed**, CCI Symposium, April 2024
- **M. Al Islam** et al., **An Adaptive Smart Water Distribution Control System for the OpenCity Testbed**, Inaugural CCI Symposium, April 2022
- **M. Al Islam** et al., **A Game-Theoretic Model for DDoS Mitigation Strategies with Cloud Services**, IEEE NOMS, April 2022

PROFESSIONAL COLLABORATION

Developing Autonomic Security Management System for Smart Cities January, 2023 - August, 2024
Virginia Commonwealth University ECE & CS *Richmond, VA, USA*

- Developed a runtime monitoring framework combining proactive and reactive defenses to detect, analyze, and autonomously respond to cyberattacks in smart cities.

Adversarial Attack Detection in Connected Autonomous Vehicles January, 2022 - August, 2022
Virginia Commonwealth University & University of Virginia *Richmond, VA, USA*

- Designed adversarial attack detection methods for DNN maneuver classifiers in CAVs by extracting spatio-temporal features from driving data, improving detection accuracy and reducing false alarms.

TEACHING EXPERIENCE

EGRE 364: Microcomputer Systems (VCU)

Spring '24, Fall '23, Spring '23, Fall '22

- Helped students implement up-down counters, USART communication, stepper motor & line-following robots using **Keil**; graded lab assignments.

EGRE 337: Statistical Info Processing (VCU)

Spring 2024

- Graded homework assignments on statistical data processing.

EGRE 245: Advanced Engineering Programming (VCU)

Fall 2023

- Guided students in advanced C programming topics such as data pointers, structures, linked lists, stacks, and binary search algorithms.

EGRE 354: Digital Logic Design (VCU)

Spring 2023

- Assisted students in designing and constructing digital logic circuits with discrete logic and FPGAs using **Vivado**; graded lab assignments.

EGRE 454: Automatic Controls (VCU)

Fall 2022


- Graded assignments on system **stability** and **pole-zero** calculations.

SOFTWARE & TOOLS

 **Programming:** Python, C, MATLAB/Simulink, ROS, Bash/Linux

 **Frameworks:** PyTorch, TensorFlow, OpenCV, Scikit-learn, Docker, Git

 **IoT:** NVIDIA Jetson (AGX), Raspberry Pi, ZED Stereo Camera; MQTT, TCP/UDP

 **CTF:** Scapy, Wireshark, Aircrack-ng, John/Hashcat, Metasploit, Burp, sqlmap, Netcat, Volatility

AWARDS & CERTIFICATIONS

- **Diamond Badge** (97th Percentile) – [NCL CTF 2025](#)
- **3rd Place** – [WVU AI Symposium 2025](#)
- **Best Poster Award** – [IEEE SmartComp \(2024\)](#)

REVIEWER RESPONSIBILITIES

- | | |
|---|--|
| • IEEE Robotics and Automation Letters (RA-L) | • Elsevier Computer Networks Journal |
| • IEEE Transactions on Network and Service Management | • IEEE International Conference on Computational Intelligence and Communication Networks (CICN) 2023 |

LEADERSHIP & SPECIAL SKILLS

- | | |
|--|--|
| • President , WVU Bengali Students' Association (BSA), Aug 2024 – Present | VCU, Spring 2023 – Fall 2023 |
| • Founding President , Bengali Cultural Association of Graduate Students (BCAGS), | • Event Coordinator , Engineering Graduate Student Association (EGSA), VCU, Fall 2021 – Spring 2022 |

REFERENCES

Available upon request.