NATIONAL CENTER FOR TRANSPORTATION CYBERSECURITY AND RESILIENCY

A USDOT National University Transportation Center

Semi-Annual Progress Report

Submitted to: United States Department of Transportation (USDOT), Office of the Assistant Secretary for Research and Technology (OST-R)

Federal Grant number: 69A3552344812, 69A3552348317

Project Title: National Center for Transportation Cybersecurity and Resiliency (TraCR)

Center Director: Mashrur "Ronnie" Chowdhury, Ph.D., P.E., F.ASCE
Eugene Douglas Mays Chair of Transportation
Clemson University, SC 29634
864-656-3313 (Phone), Email: mac@clemson.edu

Submission Date: April 30th, 2025
DUNS#: 0426298
EIN#: 57-6000254

Recipient Organization: Clemson University, Clemson, South Carolina 29634
Grant Period: June 1st, 2023 – May 31st, 2029
Reporting Period: October 1st, 2024 – March 31st, 2025
Report Term: Semi-annual

1. **ACCOMPLISHMENTS:**

1.1. What are the major goals and objectives of the program?

The mission of our "National Center for Transportation Cybersecurity and Resiliency," or TraCR, is to contribute to an ironclad defense for the nation's transportation systems against cyberattacks. The primary goal of TraCR is to address the vulnerabilities of today's and tomorrow's transportation cyber-physical systems (TCPS) holistically. TraCR continuously monitors the fast-moving world of TCPS cybersecurity, identifying challenges and threats as they appear across transportation modes, geographies, and applications.

TraCR's foundational research project is dedicated to developing a systems platform integrating hardware and software security to protect our nation's transportation infrastructure (as presented in Figure 1). Once deployed, the TraCR systems platform will be used to conduct an in-depth vulnerability assessment of any transportation system or infrastructure, followed by the identification, development, and deployment of customized security and privacy solutions for that system or infrastructure. As threats evolve and, over time, newer ones emerge, the methods and tools within the TraCR systems platform will be continuously updated with new defense strategies. The systems platform will thus serve as a reference architecture and design blueprint for developing future secure and resilient transportation systems. TraCR also researches the following four thrusts, the products and outcomes of which will support the development of the TraCR systems platform:

- Security and Resilience,
- User and Data Privacy,
- Society and Economy, and
- Evolving Quantum Computing Threats and Opportunities.

In addition to the foundational project described above, our goal is to support multiple research projects in the four thrust areas through a competitive funding program across all partner universities. The selected projects must span from fundamental research to creating ready-to-deploy and cost-effective products, procedures, and policies that are analyzed to ensure their benefits far exceed their costs. Many of these are meant to be tested at existing testbeds at our member institutions and piloted in the communities using TraCR members' proven technology transfer expertise.

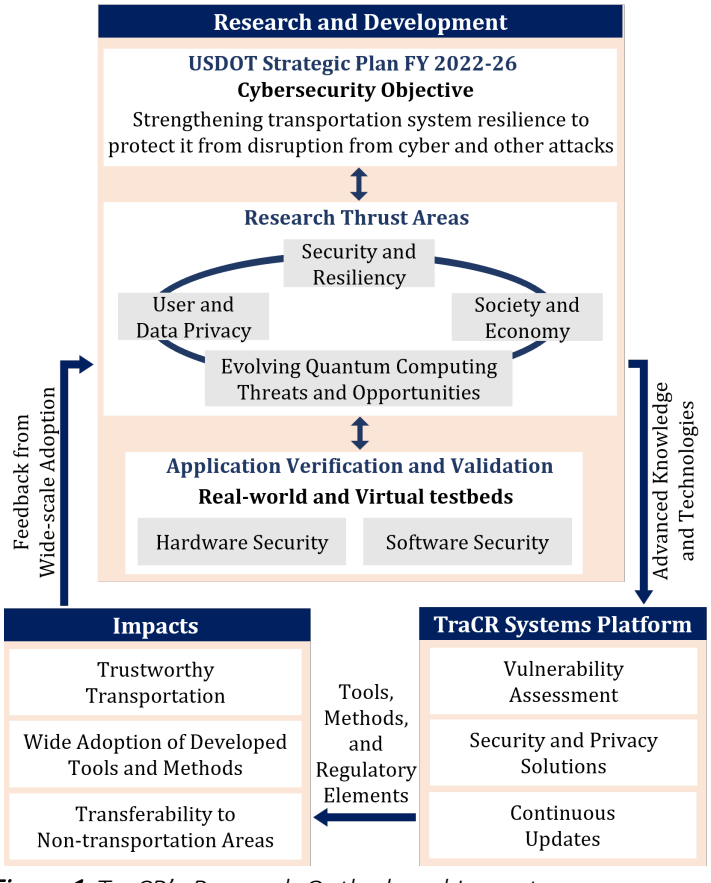

Figure 1. TraCR's Research Outlook and Impacts.

1.2. What was accomplished under these goals?

We report accomplishments across three defined categories: 1) administrative accomplishments, 2) accomplishments related to the foundational project, and 3) accomplishments related to competitively selected research projects.

1) Administrative accomplishments:

- We continued monthly web meetings with the center's leadership (Board of Directors and administrative staff) to discuss TraCR's overall progress, upcoming activities, and foundational project planning, including

input from selected faculty and students on plans, task assignments, and progress.

- We also hosted an Advisory Board meeting attended by TraCR Director Dr. Ronnie Chowdhury and all Associate Directors from partner institutions, during which the Board provided valuable feedback on current efforts and suggestions for future research and industry partnerships.

2) Accomplishments related to the foundational project:

All nine TraCR partner institutions are collaborating on the foundational project, which focuses on developing an engineered platform to contribute to the cybersecurity and resilience of the nation's transportation and infrastructure cyber-physical systems (CPS) against known and unknown threats. Key accomplishments to date include:

- TraCR researchers developed the Transportation Cybersecurity and Resiliency Threat Modeling Framework (TraCR-TMF), a semi-automated framework leveraging large language models (LLMs) to perform threat modeling tasks. TraCR-TMF systematically identifies system-level vulnerabilities, potential attack paths, and associated techniques that could compromise critical assets in transportation and infrastructure CPS applications. It enables: (i) identification of threats and their categories (e.g., spoofing, tampering, repudiation, information disclosure, denial-of-service, and elevation of privilege) based on the STRIDE model; (ii) identification of known attack techniques and their existing detection and mitigation strategies using the MITRE ATT&CK framework; and (iii) mapping of potential attack paths and techniques for each step of exploitation targeting specified critical assets. Additionally, TraCR-TMF incorporates three alternative LLM-based approaches for identifying attack techniques, varying by the level of human intervention required: (i) a retrieval-augmented generation (RAG) approach requiring no human intervention; (ii) an in-context learning approach requiring minimal human input; and (iii) a supervised fine-tuning approach requiring moderate human intervention to establish a list of relevant techniques for model training. While the RAG approach minimizes human input, supervised fine-tuning offers the best performance. These alternatives make TraCR-TMF adaptable to varying levels of professional involvement and resource availability.
- TraCR researchers developed TriSimX, a co-simulation platform that integrates a microscopic traffic simulator (SUMO), a high-fidelity 3D environment and sensor simulator (CARLA), and a network communication simulator (OMNeT++) to support comprehensive testing and validation of cybersecurity and resilience in connected and autonomous vehicle (CAV) systems. Real-world testing is often limited by high costs, safety risks, and the difficulty of reproducing complex cyberattack scenarios. TriSimX overcomes these challenges by providing a safe, scalable, and cost-effective virtual environment for evaluating cyber-physical interactions and defense strategies.
- TraCR researchers identified cyber threats targeting information flows in several service packages from the national intelligent transportation systems (ITS) reference architecture (ARC-IT) and provided recommended cybersecurity controls and mitigation strategies. This comprehensive effort included: (i) delineating and describing the components and information flows of selected ITS applications; (ii) identifying potential cyberattacks and techniques for each component and flow using the MITRE ATT&CK framework; (iii) recommending mitigation measures for the identified techniques based on the MITRE ATT&CK framework; and (iv) recommending additional cybersecurity controls based on NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations.

3) Accomplishments related to competitively selected research projects:

Seventeen new research projects were selected for funding from 23 proposals submitted in response to TraCR's Fall 2024 Request for Proposals, following external peer review. Principal investigators (PIs) were notified in December 2024, and all projects were launched on January 1st, 2025. To promote collaboration, each project involves at least one partner institution in addition to the lead institution. Aligned with TraCR's mission, these projects target cybersecurity and resilience in CAV systems, focusing on cyber threats, adversarial attacks, and AI-driven vulnerabilities. Full project details are available on the TraCR website: https://www.clemson.edu/cecas/tracr/research/projects/index.html.

Selected projects for Year 2 are shown in the following table:

No.	Proposal Title and Lead PI	Co- PI's
1.	Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems PI: Trayce Hockstad, University of Alabama (UA)	Mizanur Rahman, UA Steven Jones, UA Latifur Khan, University of Texas, Dallas (UTD) Bhavani Thuraisingham, UTD Ronnie Chowdhury, Clemson M. Sabbir Salek, Clemson Sagar Dasgupta, UA
2.	High-Fidelity Attack Modeling and Resilience Analysis of Autonomous Vehicle Software Stack PI: Z. Berkay Celik, Purdue University (Purdue)	Alvaro Cardenas, The University of California, Santa Cruz (UCSC) Daniel Fremont, UCSC Satish Ukkusuri, Purdue Leilani Gilpin, UCSC Cihang Xie, UCSC
3.	Secure and Robust Machine Learning for Autonomous Driving Systems PI: Yongkai Wu, Clemson	Feng Luo, Clemson Latifur Khan, UTD Ronnie Chowdhury, Clemson Bhavani Thuraisingham, UTD
4.	Resilient Autonomous Vehicle Perception Under Adversarial Settings PI: Bing Li, Clemson	Mert Pesé, Clemson Balaji Iyangar, Benedict College (Benedict)
5.	Cyber-Physical Investigation of Autonomous Vehicle Incidents and Attacks PI: Dave (Jing) Tian, Purdue	Dongyan Xu, Purdue Chung Hwan Kim, UTD Latifur Khan, UTD
6.	Defending Object Detectors in Autonomous Vehicles Against Adversarial Attacks with Diffusion Models PI: Long Cheng, Clemson	Feng Luo, Clemson Balaji Iyangar, Benedict
7.	Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborative Approach PI: Amjad Ali, Morgan State University (MSU)	Larry Liu, MSU Blessing Ojeme, MSU Satish Ukkusuri, Purdue
8.	Vulnerability Assessment of Sensor Fusion for Transformer-based End-to-End Autonomous Driving Models PI: Pierluigi Pisu, Clemson	Balaji Iyangar, Benedict Gurcan Comert, Benedict
9.	Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents PI: Zulqarnain Khattak, MSU	Alvaro Cardenas, UCSC
10.	Experimental Evaluations and Analysis of the Impacts of Denial-of-Service (DoS) Cyber Attacks on the Performance of Connected and Automated Vehicles (CAVs) PI: Yunyi Jia, Clemson	Ardalan Vahidi, Clemson Judith Mwakalonge, South Carolina State University (SCSU) Jagruti Sahoo, SCSU Nikunja Swain, SCSU Biswajit Biswal, SCSU

No.	Proposal Title and Lead PI	Co- PI's
11.	Resilience-Enhanced Intrusion Monitoring Against Emerging and Uncertain Threats in V2X Networks PI: Lan Emily Zhang, Clemson	Chao Fan, Clemson Lingxi Li, Purdue Satish Ukkusuri, Purdue
12.	Towards Deployment-Ready Post-Quantum Cryptography Enabled V2X Communication PI: Mizanur Rahman, UA	Ahmad Alsharif, UA Sagar Dasgupta, UA Shuhong Gao, Clemson Ronnie Chowdhury, Clemson M Sabbir Salek, Clemson Ryann Cartor, Clemson Mohammadhadi Amini, Florida International University (FIU) Kemal Akkaya, FIU
13.	Cybersecurity Testbed for Connected and Autonomous Vehicles: Phase II PI: Satish Ukkusuri, Purdue	Ronnie Chowdhury, Clemson Amjad Ali, MSU
14.	Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience PI: Mizanur Rahman, UA	Sagar Dasgupta, UA Long Cheng, Clemson Ronnie Chowdhury, Clemson
15.	Investigating Driver Behavior Under Cyber-attacks in Connected Vehicle Environments PI: Mansoureh Jeihani, MSU	Mansha Swami, MSU Ehsan Mehryaar, MSU Shubham Agrawal, Clemson Dustin Souders, Clemson
16.	Towards Securing Electric Vehicle Charging Systems Against Passive and Active Attacks PI: Ahmad Alsharif, UA	Mizanur Rahman, UA Bharat Balasubramanian, UA Sagar Dasgupta, UA Ronnie Chowdhury, Clemson M Sabbir Salek, Clemson
17.	Quantum Annealing-based Optimal Identification of Vulnerable Software Components in Connected and Autonomous Vehicles PI: Jagruti Sahoo, SCSU	Judith Mwakalonge, SCSU Nikunja Swain, SCSU Biswajit Biswal, SCSU Balaji Iyangar, Benedict

Several Year 1 projects have concluded or are nearing completion. A list of Year 1 projects can be found on our website: https://www.clemson.edu/cecas/tracr/index.html. The final reports from completed projects are currently under external review and can be found on our website once published.

Highlights of the Year 2 Projects:

- **Project:** Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience **Lead PI**: Mizanur Rahman, UA; **Collaborative Institutions:** Clemson.
  The research team reviewed multi-sensor fusion strategies to detect Global Navigation Satellite System (GNSS) cyber vulnerabilities in autonomous ground vehicle navigation, laying the groundwork for future work. The primary goal was to develop a robust spoofing detection framework that integrates with existing navigation systems. The team designed a particle filter-based GNSS spoofing detection method using Inertial Measurement Unit (IMU) data, high-definition (HD) maps, and GNSS pseudorange measurements, which outperformed conventional methods. This solution will be presented at the 2025 Institute of Navigation International Technical Meeting (ION ITM) and the 2025 IEEE/ION Position Location and Navigation Symposium (PLANS).
- **Project:** Towards Deployment-Ready Post-Quantum Cryptography Enabled V2X Communication

Lead PI: Mizanur Rahman, UA; **Collaborative Institutions:** Clemson, FIU.
The UA team advanced the deployment-readiness of post-quantum cryptographic (PQC) algorithms in secure V2X communication framework. This project evaluates PQC feasibility in operational vehicular ecosystems and develops a simulation environment for cyber-physical testing. The team began constructing a co-simulation platform integrating SUMO (traffic simulation), CARLA (3D sensor and environment simulation), and OMNeT++ (network simulation) to model complex mobility scenarios and PQC-enabled security protocols. This platform enables robust assessment of cryptographic defenses against advanced cyberattacks in V2X systems, supporting future deployment in next-gen vehicular infrastructures. Key findings were presented at the 2025 TRB Annual Meeting, Washington, D.C., in Lectern Session 2083: Risk Management—Is Artificial Intelligence a Threat or Opportunity Within Transportation Cybersecurity.

- **Project:** Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems
  Lead PI: Trayce Hockstad, UA; **Collaborative Institutions:** Clemson, UTD.
  During this reporting period, the team completed Phase I of the TraCR AI, which is a domain-specific LLM, by creating a comprehensive database of U.S. state and federal cybersecurity legislation related to transportation, and improving model output by reducing hallucinations and enhancing consistency. A preliminary analysis of the database revealed significant inconsistencies and gaps across jurisdictions, highlighting the need for a better-coordinated, transportation-aware legislative framework. These findings were shared through various academic and technical channels. Additionally, the team finalized and validated two stakeholder surveys—one for Metropolitan Planning Organizations (MPOs) and community agencies, and the other for state Departments of Transportation (DOTs)—after expert feedback.
- **Project:** Towards Securing Electric Vehicle Charging Systems against Passive and Active Attacks
  Lead PI: Ahmad Alsharif, UA; **Collaborative Institutions:** Clemson.
  During the reporting period, the research team developed a Python-based simulation of the Signal Level Attenuation Characterization (SLAC) protocol and ISO 15118 with integrated secure key establishment. The goal is to implement a proactive defense against PLC side-channel eavesdropping in EV charging. The framework enabled analysis of secure key exchange during SLAC discovery and supports future enhancements to EV communication standards.
- **Project:** High-Fidelity Attack Modeling and Resilience Analysis of Autonomous Vehicle Software Stack
  Lead PI: Z. Berkay Celik, Purdue; **Collaborating Institutions:** UCSC.
  This project aims to enhance the resilience of autonomous vehicle (AV) systems against unforeseen critical conditions caused by adversarial physical attacks. The project quantifies and improves AV resilience by exploring adversarial inputs that trigger vulnerabilities. Additionally, the project will contribute to workforce development and public awareness and inform policymakers on physical attack risks to AVs. The research team is working on four research directions: creating attacks and scenarios in AV simulation software, narrowing input space, mutating inputs based on distance and neuron coverage metrics, and analyzing input sequences triggering property violations. Key tasks include high-fidelity attack modeling and scenario generation, property-aware test oracle development, distance and neuron coverage-guided mutation engine construction, and resilience analysis, with progress underway on these deliverables.
- **Project:** Cyber-Physical Investigation of Autonomous Vehicle Incidents and Attacks
  Lead PI: Jing Tian, Purdue; **Collaborating Institutions:** UTD.
  During the reporting period, several key accomplishments were achieved. Work was conducted on investigating incidents and attacks targeting autonomous vehicles, with prototyping efforts carried out using the Robot Operating System (ROS). Research also focused on attacks originating from peripheral interfaces such as Bluetooth and USB, including the collection of Common Vulnerabilities and Exposures (CVEs) related to peripheral security within the Linux kernel. In addition, significant progress was made in uncovering bugs and vulnerabilities in Bluetooth host stacks within operating system kernels, specifically the Linux kernel and Zephyr RTOS. This research, which uncovered 31 previously unknown bugs, resulted in 9 CVEs being assigned.

- **Project:** Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborative Approach
  Lead PI: Amjad Ali, MSU; **Collaborative Institutions:** Purdue.
  During this reporting period, several milestones were achieved supporting this project. The Institutional Review Board (IRB) application process for conducting interviews was completed, and the study received an exemption under 45 CFR 46.104(d)(2) from the MSU IRB. A list of 10 potential interview subjects was identified, and two interviews were successfully conducted and completed. In parallel, the survey instrument was drafted, and relevant data sources were identified to support the research.
- **Project**: Investigating Driver Behavior Under Cyber-Attacks in Connected Vehicle Environments
  Lead PI: Mansoureh Jeihani, MSU; **Collaborative Institutions:** Clemson.
  A comprehensive literature review was completed in this reporting period, focusing on human factors in CAV cybersecurity and simulation-based driver behavior studies. Representative simulation networks for an urban environment, specifically Baltimore, were identified and finalized using driving simulators at MSU. Additionally, collaboration was initiated between partner institutions, and a synchronized experimental design framework was outlined to ensure consistency across all simulators involved in the project.
- **Project:** Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents
  Lead PI: Zulqarnain Khattak, MSU; **Collaborating:** UCSC.
  The project focused on temporal dependencies among vehicle trajectories and using real-world data from cooperative driving experiments to monitor the state of cooperative driving and detect anomalies as opposed to normal operation. For this project, the team led by MSU has utilized one set of field experiments from the Aberdeen Center in Maryland to emulate cyberattacks and study the resilience of cooperative driving. The team has tested the robustness of several algorithms and found the results to be satisfactory in anomaly detection.
- **Project:** Resilient Autonomous Vehicle Perception under Adversarial Settings
  Lead PI: Bing Li, Clemson; **Collaborating Institutions:** Benedict.
  During this reporting period, several significant accomplishments were achieved. A foundational survey explored stakeholder perspectives on adversarial threats in autonomous vehicle perception systems, initiated through collaboration with Dr. Iyangar and his student at Benedict. This survey is key to identifying real-world concerns and guiding future research. Additionally, robust and accurate camouflage generation attacks on object detection modules were reproduced and tested in the CARLA simulation environment to assess the impact of physical adversarial perturbations. The team also reproduced and analyzed Dirty Road Patch (DRP) and shadow-based attacks on lane detection and traffic sign recognition systems in offline testing environments. A preliminary vulnerability analysis of perception models, such as YOLO, under physical adversarial scenarios revealed accuracy degradation in detection and recognition tasks. The team to assemble a curated dataset of adversarial examples for future training and robustness evaluations.
- **Project:** Vulnerability Assessment of Sensor Fusion for Transformer-based End-to-End Autonomous Driving Models
  Lead PI: Pierluigi Pisu, Clemson; **Collaborating Institutions:** Benedict.
  During the reporting period, several key accomplishments were achieved. The TransFuser and InterFuser models were successfully implemented in the CARLA simulator environment, laying the groundwork for vulnerability assessment research. Both models were validated on the CARLA Autonomous Driving Leaderboard, where documented performance metrics revealed significant differences in their capabilities, with the TransFuser achieving a driving score of 61.99% and the InterFuser scoring 79.95%. Additionally, the development of a comprehensive evaluation framework was initiated, which will facilitate consistent testing of both models under identical conditions to ensure a fair comparison of their vulnerabilities.

1.3. What opportunities for training and professional development has the program provided?

Our training and professional development activities for the reporting period are reported below as organized into one of four categories: 1) webinars, 2) workshops, and 3) courses.

1) Webinars

- TraCR hosts monthly webinars from experts in the transportation sector or from TraCR researchers. Recordings for all webinars are available on our YouTube channel. (https://www.youtube.com/@TraCR-UTC). Speakers hosted during the reporting period include:
  - Dr. Z. Berkay Celik, Assistant Professor, Purdue University, **Towards Compositional Secure Autonomy: From Perception to Control** (October 2024).
  - Dr. Kemal Akkaya, Professor, Florida International University, **Leveraging Generative AI for Sensor Data Falsification on Drones and Automated Vehicles** (November 2024).
  - Dr. M. Sabbir Salek, Senior Engineer, TraCR, Clemson University, **Cyber Resilience in Transportation: Navigating Quantum Computing Threats and Opportunities** (March 2025).

2) Workshops

- Jean Michel Tine (Clemson), in collaboration with Benedict, led a hands-on workshop in October 2024 for Benedict's Capstone Program, introducing participants to Pytorch, data loading, preprocessing, and building/evaluating a Convolutional Neural Network.
- Sefatun Noor-Puspa (Clemson), in collaboration with Benedict, led workshops in October 2024 and in February 2025 for Benedict's Capstone Program on Introduction to Hardware Implementation on FPGA Board Using Vivado, covering digital circuit design and basic logic circuits.
- Jean Michel Tine (Clemson), in collaboration with Benedict, led the TraCR Cybersecurity Workshop on Anomaly Detection using Deep Learning techniques on February 5th, 2025, for Computer Science Seniors at Benedict. Dr. Chowdhury also spoke at the workshop focusing on how emerging technologies like quantum computing and LLMs can reinforce cybersecurity solutions.

3) Courses

- Dr. Hadi Amini (FIU) integrated a cybersecurity module in his large undergraduate course with 179 students to expose more students to cybersecurity foundations.
- Dr. Long Cheng (Clemson) and his group developed an education module on Zero Trust (https://moaldeen.github.io/Zero_trust_website/), which provides a comprehensive overview of the Zero Trust model, including its theoretical foundation, key components, and practical implementation strategies. Dr. Cheng's team has integrated the Zero Trust module in the course CPSC 4200/6200 - Computer Security Principles.
- Dr. Mizanur Rahman (UA) led a team that developed three classroom-ready modules focused on GPS spoofing and cybersecurity navigation for Alabama teachers, under the SciREN program for K12 educational outreach. These modules are designed to support STEM instruction and introduce students to real-world transportation security concepts.
- The Purdue team developed a new course in hardware security (CS59200-HWS) in the Department of Computer Science at Purdue. The course is a grad-level intro to hardware security and focuses on real-world embedded systems and hardware hacking. The course was offered for Spring 2025 and will be offered again for Fall 2025.

1.4. How have the results been disseminated? If so, in what way/s?

- The center maintains its website at https://www.clemson.edu/cecas/tracr/ to share results and outcomes, including a list and abstract of competitively selected projects, quarterly project reports, and the center's newsletter. Key information is also disseminated via various social media outlets:
  - LinkedIn: http://www.linkedin.com/company/tracr-usdot-utc
  - X: https://x.com/tracr_utc
  - YouTube: https://www.youtube.com/@TraCR-UTC

- Several publications (published/accepted) in books and journals, and conference papers and/or presentations were contributed by TraCR-affiliated faculty members and students during the reporting period. A detailed list is provided in the Outputs section.
- TraCR researchers also delivered several keynote/invited presentations to disseminate research results and took part in panels. A list of these is given below:
  - Dr. Ronnie Chowdhury attended the International Alliance for Mobility Testing and Standardization (IAMTS) General Assembly on October 14th, 2024, as the lead for their cybersecurity thrust.
  - Dr. Ronnie Chowdhury (Clemson) participated as part of a panel discussion for the Oklahoma Transportation Research Day (OTRD) on AI in Transportation: Opportunities and Challenges on October 15th, 2024.
  - Dr. Ronnie Chowdhury (Clemson) participated as part of the panel discussion where the experts discussed cybersecurity issues related to autonomous trucks, including threats, risk management and recovery options and strategies, and the roles of government in collaboration with private industries at the North Dakota State University Autonomous Trucking Conference on October 17th, 2024.
  - Dr. Ronnie Chowdhury and Jean Michel Tine (Clemson) visited Claflin University on October 17th, 2024, for their Graduate and Professional School Visitation Day to talk about careers in cybersecurity. Dr. Chowdhury encouraged the students to explore careers in science, technology, engineering, and math, showing them how these fields offer exciting opportunities.
  - Dr. Ronnie Chowdhury (Clemson) participated as a panelist at the CYBER-CARE Symposium, on a discussion on "Securing Transportation Cybersecurity in the Digital Age" and another panel discussion on "The Transportation Center Management, Best Practice/Lessons Learned and Future" on October 18th, 2024.
  - Dr. Ronnie Chowdhury (Clemson) was a webinar speaker for the Computer Science department at FIU on October 18th, 2024, and gave a talk on Cyber-Physical Systems and Its Security and Resiliency.
  - Dr. Ronnie Chowdhury (Clemson) was a webinar speaker at MSU on November 12th, 2024. His talk focused on "Quantum Information Systems and its Opportunities."
  - Dr. Alvaro Cardenas (UCSC) gave a keynote speech titled "Physics and Security: Then and Now" at the ACM 6th Workshop on CPS & IoT Security and Privacy, on November 19th, 2024.
  - Dr. Bhavani Thuraisingham (UTD) delivered keynote presentations on AI for Transportation Systems Security at the New York Institute of Technology and Fordham University in November 2024.
  - Dr. Shaozhi Li (Clemson) participated in the Southeast Quantum Workshop, University of Tennessee, Knoxville, in November 2024
  - Dr. Bhavani Thuraisingham (UTD) delivered an ACM Fellow Distinguished Lecture on AI for Transportation Systems Security at the New Jersey Institute of Technology in November 2024.
  - Dr. Bhavani Thuraisingham (UTD) was a panelist at the IEEE Big Data Conference Workshop on Big Cyber, December 2024, on Big Data and AI: How they benefit each other.
  - Dr. Alvaro Cardenas (UCSC) gave an invited seminar at the UC Davis Institute of Transportation Studies on January 17th, 2025. His talk was titled "Preventing, Detecting, and Responding to Attacks in Autonomous Vehicles."
  - Dr. Bhavani Thuraisingham (UTD) delivered keynote presentations on AI for Transportation Systems Security at the University of Pittsburgh in January 2025 and at Arizona State University in February 2025.
  - Dr. Ronnie Chowdhury was a speaker at Benedict in February 2025. His talk to the attendees emphasized the critical role quantum computing in the future of cybersecurity technology.
  - Dr. Bhavani Thuraisingham (UTD) delivered a keynote presentation on AI for Transportation Systems Security at the University of Southern California, March 2025.
  - Dr. Alvaro Cardenas (UCSC) gave an invited talk titled "Results from International Cooperative Research in Cyber-Physical Systems Security" at the Department of Homeland Security US/Sweden Technical Exchange conference on March 11th, 2025.

- In addition to the publications and conference presentations, several technology demonstrations were conducted by TraCR researchers, as summarized below:
  - In collaboration with the IEEE ITSS Student Chapter, TraCR members at Clemson visited the Clemson Cybersecurity Operations Center on November 8th, 2024. The opportunity provided the students with the opportunity to see behind the scenes how the digital infrastructure is protected and how real-time cyber threats are handled, along with ensuring data security.
  - The Clemson team hosted a live tech demo for BMW leaders on November 13th, 2024, showcasing hybrid classical-quantum deep learning models for detecting adversarial attacks in traffic sign classification.
  - On January 23rd, 2025, the Clemson team presented a technology demonstration at Clemson Elementary School's Science, Technology, Engineering, Art, and Mathematics (STEAM) Night, inspiring students to pursue careers in STEAM.
  - Ms. Trayce Hockstad (UA) held a panel on AI and the Law on February 6th, 2025, for pre-law and law students, exploring AI, cybersecurity, and legal frameworks, leading to the onboarding of six students for Year 2 projects.
  - Dr. Mizanur Rahman (UA) participated in Transportation Awareness Day at Greensboro Middle School on February 19th, 2025, promoting cybersecurity and sustainable transportation careers to K-12 students and educators.
  - Trayce Hockstad (UA) consulted with the Alabama Department of Transportation (ALDOT) in March 2025 to refine a stakeholder survey and gather feedback on cybersecurity support needs, with ALDOT expressing interest in the project's transportation-specific large language model.
  - To celebrate CE Engineer Week 2025, TraCR members at Clemson, in collaboration with the Clemson ITE Student Chapter, hosted a live tech demonstration on February 19th, 2025. These demos showcased the integration of emerging technologies into civil engineering infrastructure.
  - On March 7th, 2025, Clemson hosted live demo featuring a guest speaker from Emory University. TraCR members presented solutions such as pedestrian safety alerts, video-based collision warnings, hybrid classical-quantum models for detecting adversarial attacks on autonomous vehicle vision systems, hardware trojan activation analysis, and CRYSTALS-Kyber–based secure key exchange.

1.5. What will you do during the next reporting period to accomplish the goals and objectives?

For the next reporting period, our proposed activites are shown below, organized into three categories: 1) plans for training, professional development, and outreach, 2) plans for the foundational project, and 3) plans for competitively selected research projects.

1) Plans for Training, Professional Development, and Outreach

- We plan to continue our monthly webinar series. The next two scheduled webinars are:
  - Dr. Jagruti Sahoo, Associate Professor, South Carolina State University, Resilient CAV Software using Reinforcement Learning based virtualized security framework (April 2025).
  - Dr. James Lambert, Professor, University of Virginia, Hypotheses of Systems Order to Address Ambiguity and Risk in Complex Systems (April 2025).
- Dr. Ronnie Chowdhury (Clemson) will deliver a webinar on Quantum Information Science - Career and Opportunities at St. Leo University on April 1st, 2025.
- Dr. Ronnie Chowdhury will deliver a keynote talk on "Securing Transportation and Critical Infrastructure: How AI is Shaping Cybersecurity Challenges and Solutions" at the AI symposium at Clemson University on April 17th, 2025.
- Dr. M Sabbir Salek (Clemson) will deliver a podium presentation on Cybersecurity in Transportation: Navigating Quantum Computing Opportunities at the 2025 SC EPSCoR Annual State Conference, on April 4th,2025 in Columbia, SC.

- Dr. Hadi Amini (FIU) along with Dr. Ronnie Chowdhury (Clemson), and TraCR Faculty Scholars Drs. Akkaya and Uluagac will serve as editors for an upcoming book on Artificial Intelligence for Cyber-physical Systems Security and Resilience to be published by Springer.
- Dr. Long Cheng will give a talk on "Security and privacy in smart home and cyber-physical systems" at the 2025 Workshop on Interdisciplinary Research on Cyber-Physical Systems: Applications, Security, and Education, in Blacksburg, VA, on April 4th, 2025.
- Abyad Enan (Clemson) will present a poster on "A GAN-based defense strategy for adversarial patch attack resilient traffic sign classification for autonomous vehicles" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Abdullah Mamum (Clemson) will present a poster on "Optimizing lattice-based signatures for secure and efficient ITS applications against an SVD-based BDD attack" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Araf Rahman (Clemson) will present a poster on "Digital twin-based real-time curve speed warning system using physics simulation" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Jean Michel Tine (Clemson) will present a poster on "False information attack detection in a connected vehicle environment with quantum-inspired long short-term memory" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Mohammad Imtiaz Hasan (Clemson) will present a poster on "Cache-based side channel attack on critical ITS infrastructure" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Sefatun Noor-Puspa (Clemson) will present a poster on "Side channel power analysis-based non-invasive detection of hardware trojans in cyber-physical systems" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Ostonya Thomas (Clemson) will present a poster on "Cybersecurity in transportation systems: policies and technology directions" in Columbia, SC, at the 2025 SC EPSCoR Annual State Conference, on April 4th, 2025.
- Dr. Ronnie Chowdhury will deliver a webinar on "Next Frontiers in Transportation and Infrastructure Cyber-Physical Systems and Their Security" at North Carolina State University on May 5th, 2025.
- Dr. Alvaro Cardenas (UCSC) and Dr. Leilani Gilpin (UCSC) will develop a summer course for high-school students focusing on the security of autonomous systems such as self-driving vehicles. https://cosmos.ucsc.edu/clusters/cluster-13/. The first iteration of this course will be in July 2025.
- The UCSC team is working to create a benchmark and then a system to evaluate when autonomous systems are taking risky actions according to the MITRE ATT&CK framework. They will be presenting their work at an OpenAI security conference in May 2025.
- The UA team plans to expand outreach to high school students via the SciREN program for K12 educational outreach, to foster early interest in transportation careers and transportation cybersecurity.
- Dr. Mizanur Rahman (UA) will participate in the National Summer Transportation Institute, an FHWA-funded residential program designed to introduce high school students to careers in transportation through immersive learning experiences.
- Dr. Z. Berkay Celik (Purdue) will serve as general chair of the Symposium on Vehicle Security and Privacy (VehicleSec) 2025, scheduled for August 11–12, 2025, at the Seattle Convention Center. This platform will support the dissemination of findings from Dr. Celik's competitively selected project, with plans to promote TraCR's transportation cybersecurity and resiliency goals through a lightning talk and a tutorial on AV security. This outreach will engage key stakeholders in the automotive security community and foster adoption of secure AV technologies, aligning with VehicleSec's mission to address security and privacy challenges across different modes of transportation.
- Dr. Mizanur Rahman (UA) will present on Cyber-resilient GNSS-based autonomous vehicle navigation at the Automotive Cybersecurity Summit 2025 in Orange County, CA, from September 8–9, 2025.
- Dr. Mizanur Rahman (UA) will be part of the panel discussion in Panel 1: Securing the Software-Defined

Vehicles – Challenges and Solutions at the Automotive Cybersecurity Summit 2025 in Orange County, CA, from September 8–9, 2025.

- Trayce Hockstad (UA) is developing an upper-level undergraduate course on Fourth Amendment Jurisprudence, which teaches the methods and research from this project in its cybersecurity and law section (to be taught in Fall 2025).
- Trayce Hockstad (UA) will be engaging a wide range of students to participate in the next steps of a competitively selected project. The project already includes a team of three undergraduate pre-law students, three current law students, two engineering Ph.D. students, and, with the goal of adding several computer science graduate students this summer.
- Trayce Hockstad (UA) plans to continue to engage state DOTs through the survey process and through demos of the LLM when it is operational.
- Trayce Hockstad (UA) plans to incorporate the research results into a pre-law curriculum at the undergraduate level.
- For Fall 2025, CS59200-HWS will be offered again at Purdue, with a focus on: (i) Covering low-level vehicle security, (ii) CAN security, ECU firmware analysis, and (iii) Covering drone security.

2) Plans for the Foundational Project:

- TraCR researchers will concentrate on several key areas moving forward. They will customize LLMs to deliver accurate, context-aware responses across various cybersecurity and transportation categories. Efforts will also focus on developing a more user-friendly, interactive LLM-powered platform to simplify access to threat intelligence and improve usability for researchers, practitioners, and policymakers. Additionally, the team will work on expanding the dataset and refining attack classification models to enhance the accuracy and adaptability of threat mapping for transportation and infrastructure CPS applications.
- In addition, TraCR researchers will focus on expanding and utilizing the TriSimX co-simulation environment to support advanced cybersecurity and resiliency testing for CAVs. Planned activities include the development of new applications that demonstrate cyberattack detection and mitigation strategies within the simulation platform, as well as integrating additional modules to increase the system's fidelity and flexibility. These enhancements will enable more comprehensive experimentation with cyber-physical threats and response mechanisms in a safe, virtual environment. The team will also continue to refine the platform's usability and scalability, making it more accessible for broader research and educational use across TraCR-affiliated institutions.
- TraCR researchers will begin developing a database to support CAV threat modeling and attack path identification by leveraging topic modeling, LLMs, and open-source data from GitHub repositories, news articles, and existing academic literature. This work aims to establish a structured, dynamic threat knowledge base that can be integrated with simulation and analysis tools to support real-time scenario generation, risk assessment, and decision-making frameworks.

3) Plans for Competitively Selected Projects:

Plans for selected projects for Year 2 are highlighted below:

- **Project:** Safe and Reliable Autonomous Vehicle Navigation through Cyber Resilience
  Lead PI: Mizanur Rahman, UA; **Collaborative Institutions:** Clemson.
  The team will finalize a systematic literature review and develop a detailed threat model targeting GPS vulnerabilities, with emphasis on the control segment. The team will design and implement spoofing detection and mitigation algorithms using loosely coupled sensor fusion that integrates GNSS, IMU, and perception sensors. The team will also develop a trustworthy monitoring module leveraging TEEs to enable secure navigation decision-making for autonomous vehicle systems.
- **Project:** Towards Deployment-Ready Post-Quantum Cryptography Enabled V2X Communication
  Lead PI: Mizanur Rahman, UA; **Collaborative Institutions:** Clemson, FIU.

The project will design quantum-resilient cryptographic protocols for V2X communications, beginning with lightweight post-quantum digital signature algorithms optimized for constrained vehicular environments. The team will also implement a certificate segmentation strategy to reduce message and certificate size, ensuring compatibility with the IEEE 1609.2 security framework. Additionally, they will develop a federated learning-enabled co-simulation platform integrating CARLA, SUMO, and OMNeT++ to assess the performance of PQC-enabled V2X systems under realistic traffic and attack scenarios. These efforts aim to enable secure, scalable PQC deployment in future transportation systems.

- **Project:** Cybersecurity Analysis and Guidance to Support Secure Transportation Cyber-Physical Systems
  Lead PI: Trayce Hockstad, UA**; Collaborative Institutions:** Clemson, UTD.
  This project will continue to refine and expand the domain-specific LLM for legal and policy analysis in transportation cybersecurity. To improve model robustness, planned efforts include curating additional data sources—specifically international legislation and academic research on data privacy and cybersecurity policy. The team will also implement methods to reduce hallucinations in the LLM's responses and finalize the distribution of stakeholder surveys to MPOs, DOTs, and community agencies.
- **Project:** Towards Securing Electric Vehicle Charging Systems against Passive and Active Attacks
  Lead PI: Ahmad Alsharif, UA; **Collaborative Institutions:** Clemson.
  In the coming reporting period, the research team will focus on securing power line communication (PLC) between electric vehicles (EVs) and charging stations against both passive eavesdropping and active interference. The research team is developing a proactive defense protocol using identity-based encryption for SLAC initialization, creating a real-time monitoring tool to detect intelligent jamming attacks, and implementing a backup communication method .
- **Project:** Cybersecurity Testbed for Connected and Autonomous Vehicles (Phase II)
  Lead PI: Satish V. Ukkusuri, Purdue; **Collaborating Institutions:** Clemson, MSU.
  This project aims to develop a physical testbed to assess the real-world network-level impact of cyberattacks on CAV fleets, expanding upon the Phase I co-simulation framework that integrated METS-R and CARLA. The research team is constructing a testbed with multiple AVs, intelligent traffic lights, and roadside sensors to support vehicle-to-infrastructure (V2I) communication. The design mirrors CARLA's virtual map for high simulation-to-reality fidelity. The team is also modeling cyberattacks on visual sensors—building on previous work—and validating them through integrated CARLA-physical testbed communication to measure their real-world effects. The team is testing additional attack types, for example, visual sensor attacks, denial-of-service, and basic safety message (BSM) manipulation, to improve both physical and software components of CAVs.
- **Project:** Defending Object Detectors in Autonomous Vehicles Against Adversarial Attacks with Diffusion Models
  Lead PI: Long Cheng, Clemson; **Collaborating Institutions:** Benedict.
  This project aims to investigate patch-agnostic and attack-agnostic defense mechanisms for object detectors in autonomous vehicles against adversarial patch attacks. The team is currently developing a diffusion-based defense, which operates through a two-stage pipeline: (1) a regeneration stage that leverages inpainting diffusion models to reconstruct images that contain adversarial patches, and (2) a rectification stage that detects and replaces adversarial patches with benign content.
- **Project:** Increasing Cybersecurity Workforce in the Transportation Systems Sector: An Interdisciplinary and Collaborative Approach
  Lead PI: Amjad Ali, MSU; **Collaborating Institutions:** Purdue.
  During the next reporting period, the team will focus on identifying the remaining interview subjects and conducting web scraping from the previously identified data sources. Collaboration with the project partner institution, Purdue, will continue, and efforts will also be directed toward conducting data analysis to advance the study.
- **Project:** Investigating Driver Behavior Under Cyber-Attacks in Connected Vehicle Environments
  Lead PI: Mansoureh Jeihani, MSU; **Collaborating Institutions:** Clemson.

During the next reporting period, the team will finalize the integration of connected vehicle system interfaces, such as safety warnings, into both simulators. They will also develop and implement falsification-based cyber-attack scenarios tailored to each simulation network environment. Participant recruitment and pilot testing will begin in preparation for full-scale data collection. Additionally, coordination meetings between partner institutions will continue to ensure alignment in methodology and analytical approaches.

- **Project:** Cyberattack Resilience in Cooperative Driving Automation Using Experimental Data and Federated Agents
  Lead PI: Zulqarnain Khattak, MSU; **Collaborating:** UCSC.
  The team will continue refining the project scope and emulating data for various cyberattacks using real-world experiments conducted at the American Center for Mobility. These efforts aim to assess the impact of cyberattacks on cooperative driving performance and stability while advancing anomaly detection architectures to support resilient cooperative driving operations. Dr. Khattak, the PI, is also working on integrating a cybersecurity module focused on cooperative driving into the *Intelligent Transportation Systems* course at MSU.

2. **PARTICIPANTS & COLLABORATING ORGANIZATIONS:**

TraCR established the following collaborations:

Clemson is collaborating with:

- South Carolina Established Program to Stimulate Competitive Research (SC EPSCoR)
- South Carolina Department of Transportation (SCDOT)
- South Carolina Research Authority (SCRA)
- International Alliance for Mobility Testing and Standardization (IAMTS)
- MITRE Corp.
- International Transportation Innovation Center (ITIC)

FIU is collaborating with

- SUNTRAX Test Facility (https://suntraxfl.com)
- Qualcomm, to get feedback on the foundational project

UA is collaborating with the following entities:

- Hexagon/NovAtel Inc., a global leader in digital reality solutions combining sensor, software, and autonomous technologies.
- Spirent Federal Systems Inc., which provided Spirent GSS9000, a hardware-in-the-loop Global Navigation Satellite Systems (GNSS) simulator package.
- Integrity Security Services (ISS), Ashburn, VA, which provided access of SCMS certificate bundles for V2X communications (In-kind support).
- Geodnet, San Francisco, CA, which provided RTK base stations for precise Positioning, Navigation and Timing (PNT) (In-kind support).
- Alabama Department of Transportation, who were consulted on survey development.

MSU is collaborating with:

- Maryland Transit, which shares its knowledge of state-of-the-art transit security management.
- Virginia Department of Transportation (VDOT) provided a cash match of $63,000 to collaborate in one of our competitive projects. They consider the project methodology and outcomes pivotal for securing the VDOT traffic operations, management centers, and connected vehicle applications against cyber vulnerabilities.
- National Security Engineering Center, a Department of Defense (DoD) funded Research and Development Center.

Purdue is collaborating with Qualcomm (Dr. Jonathan Petit and Mr. Raashid Ansari).

UCSC is collaborating with:

- University of California, Berkeley, to develop and disseminate Scenic results.

- San Jose State University for research in securing autonomous vehicles.
- Google and OpenAI, who are providing funding for part of the work aligned with TraCR.
- Toyota, Deutsche Bahn, and MaplessAI, who are active users of Scenic.

3. **OUTPUTS:**

3.1. Publications, conference papers, and presentations

1) Books, Book Chapters, and Journal Publications

Published/In-press

1. Dasgupta, S., Irfan, M.S., Rahman, M, Chowdhury, M, 2025. Chapter 15 - Detection and Mitigation of Spoofing Attacks in GNSS-Based Autonomous Ground Vehicle Navigation Systems. In: Data Analytics for Intelligent Transportation Systems, 2nd Ed., pp. 403–427, Elsevier.
2. Hockstad, T., Rahman, M., Jones, S., Chowdhury, M., 2024. A Regulatory Gap Analysis in Transportation Cybersecurity and Data Privacy. Transportation Journal, 64, e12036.
3. Shakib, K.H., Rahman, M., Islam, M., Chowdhury, M., 2025. Impersonation Attack Using Quantum Shor's Algorithm Against Blockchain-Based Vehicular Ad-Hoc Network. IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2025.3534656.
4. Ali, A., 2025. Emerging Cyberthreats to AI-Powered Cybersecurity Systems and Innovative Defense Strategies: A Comprehensive and Systematic Literature Review. *Electronics*, *in press.*

Under-review/In-preparation

1. Wang, Z., Xie, C., Bartoldson, B., Kailkhura B., 2025. Double Visual Defense: Adversarial Pre-training and Instruction Tuning for Improving Vision-Language Model Robustness. *Under review*. arXiv: 2501.09446.
2. Khandakar, A., Uddin, M., Hockstad, T., Khan, L., Rahman, M., Chowdhury, M., Salek, M., Thuraisingham, B., Jones, S., 2025. Retrieval Augmented Generation-Based Large Language Models for Bridging Transportation Cybersecurity Legal Knowledge Gaps. *Under review.*
3. Hockstad, T., Rahman, M., Chowdhury, M., Akbar, K., Uddin, M., Khan, L., 2025. Data Security & Privacy Regulation in the U.S.: A 50-State Legislative Survey. *Under review.*
4. Lei, Z., Ukkusuri., S.V., 2025 Assessing the risks of adversarial booking attack to autonomous mobility-on-demand services. Transportation Research Part C: Emerging Technologies*. Under review*.
5. Ka, E., Ukkusuri, S.V., 2025. Route Guidance Attacks in Cyber Transportation Networks: A User-Centered Study of Behavioral Sensitivity. Transportation Research Part F: Traffic Psychology and Behaviour. *Under review.*
6. Barbosa, D., Burbano, L., Hernandez, C., Lei, Z., Park, Y., Ukkusuri, S.V., Cardenas, A.A., 2025. D4+: Emergent Adversarial Driving Maneuvers with Approximate Functional Optimization. Handbook of Dynamic Data Driven Applications Systems*. Under review.*
7. Anderson J., Aldeen M., Zhang S., Liao S., Hu H., Chowdhury M., Cheng L., 2025. Zero Trust: A Survey. *In preparation.*
8. Mukwaya, A., Benibo, I., Sahoo, J., Mwakalonge, J., Gyimah, N., Comert, G., Biswal, B., Swain, N., 2025. Lidar Buffer Overflow Exploitation in Connected and Autonomous Vehicles (CAV) Software. *In preparation*.
9. Zhang, K., Salek, M.S., Wang, A., Rahman, M., Chowdhury, M., and Lao, Y. 2025. Preparing for Kyber in Securing Intelligent Transportation Systems Communications: A Case Study on Fault-Enabled Chosen-Ciphertext Attacks. Cybersecurity. *Under review*.
10. Majumder, R., Comert, G., Werth, D., Gale, A., Chowdhury, M., and Salek, M.S. 2025. Graph-Powered Defense: Controller Area Network Intrusion Detection for Unmanned Aerial Vehicles. Transportation Research Record. *Under Review*. arXiv: 2412.02539.
11. Majumder, R., Chowdhury, M., Khan, S.M., Khan, Z., Ahmad, F., Ngeni, F., Comert, G., Mwakalonge, J. and Michalaka, D. 2025. Quantum Computing Supported Adversarial Attack-Resilient Autonomous Vehicle Perception Module for Traffic Sign Classification. Intelligent Systems with Applications. *Under review*. arXiv: 2504.12644.

12. Enan, A. and Chowdhury, M., 2025. GAN-Based Single-Stage Defense for Traffic Sign Classification Under Adversarial Patch Attack. IEEE Transactions on Intelligent Transportation Systems. *Under review*. arXiv: 2503.12567.
13. Salek, M., Chowdhury, M., Tine, J.-M., Hasan, M.I., Munir, M.B., Cai, Y., Khan, L., and Rahman, M. 2025. A Large Language Model-Supported Threat Modeling Framework for Intelligent Transportation Systems Applications. *In preparation*.

2) Conference Papers/Presentations

1. Munir, M.B., Cai, Y., Khan, L., Thuraisingham B. Leveraging Multimodal Retrieval-Augmented Generation for Cyber Attack Detection in Transit Systems. Presented at the IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA), Pittsburgh, PA, October 2024.
2. Ortiz, D., Burbano, L., Cardenas, A., Xie, C., Cao, Y. Robust and Efficient AI-Based Attack Recovery in Autonomous Drones. Presented at the GENZERO Workshop, November 2024.
3. Hernandez, C., Barbosa, D.E.O., Lei, Z., Burbano, L.; Park, Y., Ukkusuri, S.V., Cardenas, A. D4: Dynamic Data-Driven Discovery of Adversarial Vehicle Maneuvers. Presented at the 5th Dynamic Data-Driven Application Systems (DDDAS) International Conference, November 2024.
4. M. Hadi Amini. Secure Federated Learning for Autonomous Transportation Systems. Presented at the 2024 International Conference on Computational Science and Computational Intelligence, Las Vegas, NV, December 2024.
5. Akbar, K.A., Uddin, M., Hockstad, T., Khan, L., Rahman, M., Chowdhury, M., Salek, M.S., Thuraisingham, B., Jones, S. Retrieval Augmented Generation-Based Large Language Models for Bridging Transportation Cybersecurity Legal Knowledge Gaps. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
6. Dasgupta, S., Irfan, M.S., Rahman, M. Transportation Landmark-Based Navigation System for Autonomous Ground Vehicles in GNSS-Contested Urban Areas. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
7. Hockstad, T., Fisher, J. Grid Modernization and Cybersecurity: Policy Implications for Electric Vehicle Infrastructure. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
8. Hockstad, T., Rahman, M., Chowdhury, M., Akbar, K., Uddin, M., Khan, L. Data Security & Privacy Regulation in the U.S.: A 50-State Legislative Survey. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
9. Ka, E., Ukkusuri, S.V. Analytical Framework for Network-Level Traffic Flow under Route Guidance Attacks: An Extension of the Generalized Bathtub Model. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
10. Ka, E., Ukkusuri, S.V. Comparative Analysis of Sampling Methods in Physics-informed Neural Networks for Traffic State Estimation in Large-scale Road Networks. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
11. Khandakar, A., Uddin, M., Khan, L., Hockstad, T., Rahman, M., Chowdhury, M. Mitigating Hallucinations in Transportation Cybersecurity Legislation Analyses. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
12. Lin, G., Qian, S., Khattak, Z.H. Cyberattack Vulnerability and Resilience of Cooperative Driving Automation Using Federated Learning. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
13. Mamun, A.A., Abrar, A., Rahman, M., Salek, M.S., Chowdhury, M. Enhancing Intelligent Transportation System Security: A Shift to Post-Quantum Cryptography. Presented at the 104th Annual Meeting of Transportation Research Board, Washington, D.C., January 2025.
14. Puspa, S., Enan, A., Majumder, R., Comert, G., Salek, M.S., Chowdhury, M A. Side Channel Power Analysis Based Stealthy Hardware Trojan Detection Method for Securing the Integrated Circuits in Transportation

Hardware. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.

15. Thomas, O., Salek, M., Tine, J., Rahman, M., Hockstad, T., Chowdhury, M. Cybersecurity in Transportation Systems: Policies and Technology Directions. Presented at the 104th Annual Meeting of the Transportation Research Board, Washington, D.C., January 2025.
16. Dasgupta, S., Rahman, M., Irfan, M.S., Ahmad, M.U. Enhanced Navigation for Autonomous Vehicles in GNSS-Denied Urban Environments: Integrating GIS with Deep LSTM/Robust Kalman Filter-Based Landmark Navigation System. Presented at the Institute of Navigation International Technical Meeting (ION ITM), Long Beach, CA, January 2025.
17. Irfan, M.S., Dasgupta, S., Rahman, M. A Particle Filter-Based Sensor Fusion Approach for GNSS Spoofing Detection Incorporating Ground Vehicle Navigation Constraints. Presented at Institute of Navigation International Technical Meeting (ION ITM), Long Beach, CA, January 2025.
18. Mukwaya, A., Sahoo, J., Gyimah, N., Biswal, B., Mwakalonge, J., Comert, G., Swain, N. Code diversity defense mechanism for Connected Autonomous Vehicles. Presented at the 2025 Annual BECT Research Symposium, Orangeburg, SC, February 2025.
19. Benibo, I., A. Sahoo, J., Gyimah, N., Biswal, B., Mwakalonge, J., Comert, G., Swain, N. Vulnerability Testing Framework for Connected and Autonomous Vehicles. Presented at the 2025 Annual BECT Research Symposium, Orangeburg, SC, February 2025.
20. Ruganuza, D., A. Sahoo, J., Gyimah, N., Biswal, B., Mwakalonge, J., Comert, G., Swain, N. A review of Cybersecurity in Connected and Autonomous Vehicles: State of the Art on Code Diversification and Future Research Directions. Presented at the 2025 Annual BECT Research Symposium, Orangeburg, SC, February 2025.
21. Benibo, I., Sahoo, J., Mwakalonge, J., Gyimah, N.K., Comert, G., Biswal, B., Swain, N. Q-Learning-Based Adaptive Defense Mechanism for Connected Autonomous Vehicles. Presented at the 2025 IEEE SoutheastCon Conference, Concord, NC, March 2025.
22. Gyimah, N.K., Mwakalonge, J., Comert, G., Siuhi, S., Akinie, R., Sulle, M., Ruganuza, D., Benibo, I., Mukwaya, A. An AutoML-based approach for Network Intrusion Detection. Presented at the 2025 IEEE SoutheastCon Conference, Concord, NC, March 2025.
23. Gerhart, A., Iyangar, B., Chowdhury, M. Saving AI from Itself: Defending Healthcare Systems Against Adversarial Threats. Accepted for presentation at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
24. Jimoh, T., Iyangar, B., Chowdhury, M. Autoencoders vs FGSM: Comparison of Machine-Learning Models for Detecting Adversarial Perturbations in Image Classification. Accepted for presentation at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
25. Mamun, A.A., Abrar, A., Rahman, M., Salek, M.S., Chowdhury, M. Future-Proofing Transportation Cyber-Physical Systems: The Role of Post-Quantum Cryptography. Accepted for presentation at the 2025 SC EPSCoR State Conference, Columbia, SC, April 2025.
26. Irfan, M.S., Dasgupta, S., Rahman, M. A Particle Filter-Based Sensor Fusion Approach for GNSS Spoofing Detection Incorporating Ground Vehicle Navigation Constraints. Accepted for presentation at the IEEE/ION Position, Location and Navigation Symposium (PLANS), Salt Lake City, UT, April 2025.
27. Wang, C., Cardenas, A., Comert, G., Kantarcioglu, M. A Systematic Evaluation of Generative Models on Tabular Transportation Data. Accepted for presentation at PAKDD: Pacific Asia Conference on knowledge Discovery and Data Mining, Sydney Australia, June 2025.
28. Cai, Y., Munir, M.B., Khan, L., Thuraisingham B. Enhancing ITS Cybersecurity with ModernBERT: Mapping Information Flows to MITRE ATT&CK Techniques. Submitted to 12th IEEE International Conference on Data Science and Advanced Analytics (DSAA), Birmingham, UK, October 2025.
29. Raze, A., Zhang, Z. CAROT: A Secure RISC-V ECU with TEEs and MTD. In preparation for submission to SecDev 2025, Indianapolis, IN, October 2025.

30. Ma J., Aldeen M., Salas C., Luo F., Chowdhury M., Pesé M., Cheng L., "DisPatch: Disarming Adversarial Patches in Object Detection with Diffusion Models. Submitted to the Network and Distributed System Security (NDSS) Symposium, San Diego, CA, February 2026.
31. Ka, E., Ukkusuri, S.V. Adaptive Spatial-Temporal Domain Decomposition in Physics-Informed Neural Networks for Traffic State Estimation. Submitted to 26th International Symposium on Transportation and Traffic Theory (ISTTT26), Munich, Germany, July 2026.

*3) **Theses and Dissertations***

1. Zengxiang Lei (Ph.D., Civil Engineering, Purdue), Towards an efficient and secure ride-hailing service.
2. Jean Michel Tine (M.S., Civil Engineering, Clemson), False Information Attack Detection in a Connected Vehicle Environment With Quantum-Inspired Long Short-Term Memory.
3. Reek Majumdar (Ph.D., Civil Engineering, Clemson), Integrating Artificial Intelligence for Transportation Cyber-Physical Systems: From Detection to Cyber Resilience.

4) Website(s) or Other Internet site(s)

- The official TraCR website (https://www.clemson.edu/cecas/tracr/) provides detailed information about the center's activities. The Research tab includes descriptions of research thrusts, annual Request for Proposals (RFPs), selected projects, and their reports.
- TraCR's X page (https://x.com/tracr_utc) is used to share updates, webinar announcements, and news with the broader transportation community and has expanded in user engagement.
- The YouTube channel (https://www.youtube.com/@TraCR-UTC) hosts recordings of all TraCR Scholar Webinars and will continue to feature videos related to the center.
- The LinkedIn page (http://www.linkedin.com/company/tracr-usdot-utc) shares updates with the professional community and posts all TraCR-related job openings to reach a wide applicant pool.

3.2. Technologies or techniques

- **CAROT:** CAROT, an open-source, cyber-resilient Electronic Control Unit (ECU) based on the RISC-V architecture developed by Clemson researchers, integrates a TEE and instruction-set randomization as a moving-target defense against code-injection and operating system attacks. Implemented on a Xilinx Field Programmable Gate Arrays (FPGA) testbed, CAROT supports UTC's low-cost reproducibility and technology transfer goals, with open-source design files. In CARLA lane-keeping simulations, CAROT incurred less than 1.1% performance overhead and a 1.05% average latency increase, which is well within industry ECU timing requirements.
- **QuanCrypt:** The FIU team advanced solutions for securing federated learning (FL) in transportation cybersecurity, leading to the development of QuanCrypt-FL. FL enables decentralized model training without sharing private data, but remains vulnerable to inference attacks like gradient inversion and membership inference. To address this, QuanCrypt-FL integrates low-bit quantization, pruning, and mean-based clipping to mitigate quantization errors, reduce computational costs, and maintain strong privacy protections. This communication-efficient framework preserves model accuracy while improving computational efficiency and attack resilience. Validation on benchmark datasets shows QuanCrypt-FL consistently outperforms state-of-the-art methods, matching Vanilla-FL accuracy while achieving up to 9x faster encryption, 16x faster decryption, 1.5x faster inference, and up to 3x faster training compared to BatchCrypt.
- **Quantum Impersonation Attack Simulation for VANETs:** A quantum-based impersonation attack model was developed by our UA researchers using IBM Qiskit and simulated in SUMO, OMNeT++, and VEINS to evaluate the vulnerability of blockchain-based vehicular networks under Shor's algorithm. This technique demonstrates the potential risk of identity spoofing in post-quantum scenarios and informs the development of quantum-resilient security protocols.
- **Particle Filter-Based GNSS Spoofing Detection Framework:** A spoofing detection method using particle filters and multi-sensor fusion (GNSS, IMU, HD maps) was designed by the UA researchers to improve

cyber-resilience in AV navigation systems. The technique demonstrated enhanced accuracy and robustness under various attack conditions and is compatible with existing vehicle systems.

- **TraCR AI – Domain-Specific Legal Language Model:** The TraCR team developed an early version of a domain-specific LLM trained on U.S. transportation cybersecurity legislation. Though still undergoing refinement to reduce hallucinations and improve reliability, the model has been successfully demonstrated and is intended for open distribution to state DOTs and MPOs once operational maturity is achieved.

3.3. Inventions, patent applications, and/or licenses

- The FIU team has filed a patent application to the USPTO, based on research partly funded by TraCR: Namrata Saha, Shabnam Rezapour, and Mohammadhadi Amini, Systems and Methods for Advancing the Restoration Process for Interdependent Critical Infrastructures, Serial Number, 19/058,257.
- The FIU team is also working with the FIU Tech Transfer Office for another invention disclosure on "A Privacy-Preserving Federated Fine-Tuned Large Language Model."

4. OUTCOMES:

There are several technical outcomes from our work so far in this reporting period:

- TraCR-TMF, an LLM-enabled automated threat modeling framework for transportation and infrastructure CPS developed by TraCR researchers, offers alternative strategies with different levels of human intervention requirements. The TraCR-TMF helps transportation professionals or associated security operation centers make informed decisions to protect their critical systems and infrastructure by identifying the system-levels vulnerabilities and the attack vectors that could be utilized to exploit them.
- The TraCR AI initiative has increased awareness of regulatory inconsistencies in transportation cybersecurity legislation across U.S. states. The legal analysis and preliminary findings, disseminated through publications and technical presentations, contribute to the growing knowledge in cybersecurity policy for transportation systems and are expected to guide future regulatory and legislative efforts. Additionally, developing this transportation-specific LLM integrating RAG has contributed to reducing LLM hallucinations and improving model reliability in legal and regulatory interpretation.
- Collaboration with ISS and other SCMS providers, alongside the development of a PQC-integrated C-V2X simulation platform, is advancing the state of practice in secure V2X communications. This outcome supports adopting next-generation cryptographic technologies in anticipation of post-quantum threats.
- Engagement with the State DOTs and the development of sector-specific cybersecurity surveys have helped ensure that research activities remain aligned with real-world operational needs. These efforts have improved awareness of industry concerns related to cybersecurity, including data protection, regulatory compliance, and operational security.

In addition, there are several other outcomes from the participation of TraCR personnel in various professional development and outreach activities:

- Dr. Alvaro Cardenas (UCSC) was elected vice-chair of the IEEE Computer Society Technical Committee on Security and Privacy and joined the steering committee of the IEEE Symposium on Security and Privacy.
- Dr. Ronnie Chowdhury serves as an expert panel member for the Government Accountability Office (GAO)'s Smart Cities and Communities initiative, providing expertise in evaluating government spending and efficiency.
- Dr. Ronnie Chowdhury served as an advisory board member for the Computer Science and Engineering Department at Benedict College for the 24-25 academic year.
- In January 2025, Dr. Ronnie Chowdhury received the Presidential Award for Excellence in Science, Mathematics, and Engineering Mentoring from the White House.
- A UCSC student team won "Challenge 1: Resilient Edge AI for Hierarchical Drone Swarms" at the GENZERO workshop in November 2024.
- MSU's cyber competition team participated in the Spectral Cloak National Cyber Competition on October 26, 2024, sponsored by MITRE and the National Security Engineering Center.

5. **IMPACTS:**

Established in 2023, TraCR is in its fourth semi-annul reporting period. Our activities have already had impacts, with ongoing progress in TraCR-supported competitively selected research projects expected to drive further impacts.

5.1. What is the impact on the effectiveness of the transportation system?

- TraCR's research on cybersecurity analysis for transportation cyber-physical systems unifies traditionally siloed fields—legal studies, AI/natural language processing (NLP), and transportation engineering—into an interdisciplinary methodology that advances cybersecurity law and policy. By synthesizing fragmented federal and state regulations into a structured, digestible framework, which enables more targeted and enforceable legislation. This reduces regulatory confusion, strengthens system resilience, and supports agile legal responses to emerging threats. Our work is drawing strong interest from diverse stakeholders, including state DOTs, TRB committees, and public and private organizations.
- Our partners at the UCSC developed Scenic—a probabilistic programming language for environment (or world) modeling and data generation for autonomous intelligent cyber-physical systems with partial support from TraCR. The Scenic repository has seen exceptional community adoption for an academic artifact, with over 320 stars and 110 forks on GitHub—placing it in the top decile of all research codebases. Notably, only 3.7% of GitHub repositories linked to top-tier software engineering papers exceed 100 stars. Scenic has also been adopted as a core environment-generation engine by widely used autonomous driving simulators such as CARLA, and by safety evaluation benchmarks like SafeBench—demonstrating strong uptake in both research and industry.

5.2. What is the impact on the adoption of new practices, or instances where research outcomes have led to the initiation of a start-up company?

- Research from TraCR's resilient autonomous navigation initiative has partially led to the creation of Resilient Timing Systems, LLC (Entity ID: 001-092-469), a start-up focused on resilient GNSS solutions for intelligent transportation systems. The company is commercializing a node-based ground mesh architecture with AI capabilities for real-time cyberattack mitigation and redundancy in GNSS-denied or spoofed environments. This architecture builds on TraCR-supported research on cyber-resilient navigation.
- Microsec, a V2X public key infrastructure (PKI) solution provider, expressed its interest in adopting TraCR's PQC-enabled security solutions into its products.

5.3. What is the impact on the body of scientific knowledge?

Nothing to report yet.

6. **CHANGES/PROBLEMS**

6.1. Changes in approach and reasons for change

Nothing to report.

6.2. Actual or anticipated problems or delays and actions or plans to resolve them

Nothing to report.

6.3. Changes that have a significant impact on expenditures

Nothing to report.

6.4. Significant changes in use or care of human subjects, vertebrate animals, and/or biohazards

Nothing to report.

6.5. Change of primary performance site location from that originally proposed

Not applicable.

7. **SPECIAL REPORTING REQUIREMENTS**

None.