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
Director, USDOT Center for Connected Multimodal Mobility (C^2M^2)
Clemson University, SC 29634
864-656-3313 (Phone), Email: mac@clemson.edu

Submission Date: October 30th, 2024
DUNS#: 0426298
EIN#: 57-6000254

Recipient Organization: Clemson University, Clemson, South Carolina 29634
Grant Period: June 1st, 2023 – May 31st, 2029
Reporting Period: April 1st, 2024 – September 30th, 2024
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 build 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-social systems (TCPSS) holistically. TraCR continuously monitors the fast-moving world of TCPSS 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 Environment, 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.

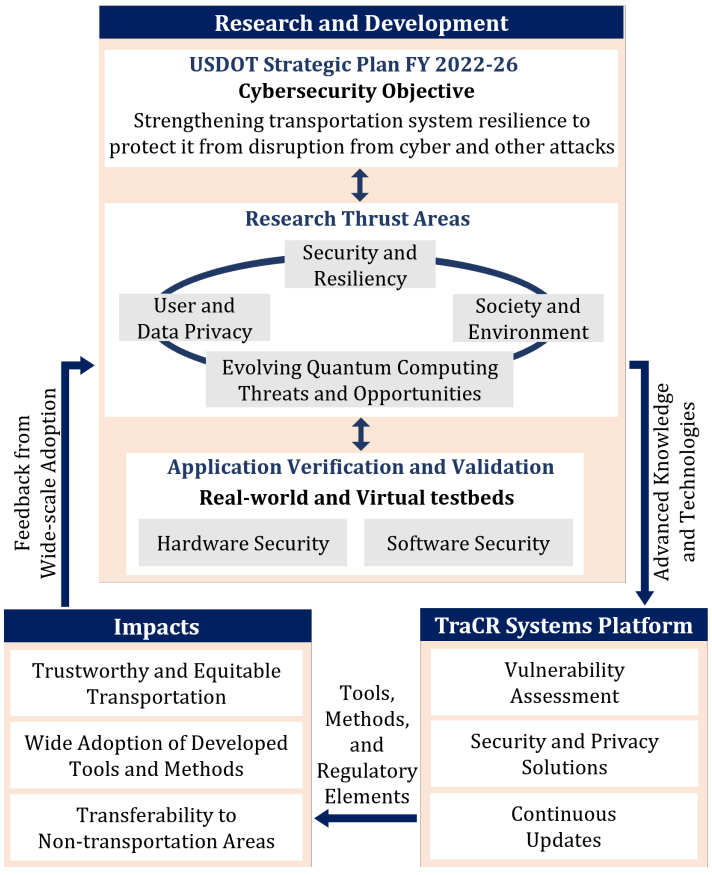

Figure 1. TraCR's Research Outlook and Impacts.

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 have continued our monthly recurring web meetings with the center's leadership (Board of Directors and administrative staff) to discuss TraCR's progress and upcoming activities.
- We have continued our monthly recurring web meeting with the center's leadership (Board of Directors and administrative staff) and selected faculty and students to discuss plans, task assignments, and progress related to TraCR's foundational project.
- A request for proposal (RFP) for competitively funded projects for Year 2 was sent to TraCR Associate Directors to disseminate to their respective institutions on August 30th, 2024. The deadline for proposal submission was October 7th, 2024. A total of 23 research proposals were received, which have been sent to reviewers for a double-blind peer review. Reviewer feedback will be received in mid-November, and we expect to make project selections by the end of November. All Year 2 funded projects will begin on January 1st, 2025.
- TraCR hosted its inaugural annual conference on May 6-7, 2024, at the Clemson University International Center for Automotive Research (CU-ICAR) campus in Greenville, South Carolina. This conference aimed to foster collaboration and innovation among leaders in transportation cybersecurity research within the nine institutions partnering on TraCR, bringing diverse groups of researchers, scholars, and professionals from the various institutions. Over two days, attendees showcased their latest research findings, presented innovative technologies, and discussed cutting-edge solutions to protect future transportation systems from the ever-growing threat of cyberattacks. The presentations underscored the critical importance of collaborative efforts in tackling the multifaceted challenges confronting our transportation infrastructure today and tomorrow. Industry leaders and government representatives also attended, and their contributions added depth and perspective to the discussions. The conference also featured technology demonstrations and poster presentations led by students and researchers to showcase their research and foster academic exchange and collaboration. Overall, the conference laid a foundation for future conferences and reaffirmed the commitment of TraCR and its consortium partners to advancing transportation cybersecurity research.
- TraCR took a pivotal role in the inaugural Future of Transportation (FoT) Summit hosted by USDOT at its headquarters in Washington, D.C., from August 13-15, 2024. The event focused on transformative research in mobility, safety, infrastructure, sustainability, and cybersecurity conducted at the University Transportation Centers, with funding from the FAST Act and the Bipartisan Infrastructure Law. TraCR personnel were closely involved in the planning and execution of the event. In addition, Dr. Ronnie Chowdhury, TraCR Director, spoke on Cybersecurity and Resiliency of Transportation Systems and Infrastructure and moderated another cybersecurity session. Other TraCR leadership team members also presented, including Dr. Bhavani Thuraisingham from the University of Texas, Dallas (UTD), who spoke on Trustworthy Artificial Intelligence for Securing Transportation Systems, Dr. Alvaro Cardenas from the University of California, Santa Cruz (UCSC), whose presentation focused on Building Blocks for Connected and Autonomous Transportation Cybersecurity, and Ms. Trayce Hockstad from the University of Alabama (UA), whose talk covered Resolving Legislative Gaps in Transportation Cybersecurity.

2) Accomplishments related to the foundational project:

- Clemson is the lead institution for the foundational project. This project aims to develop a national platform to safeguard the software and hardware related to the nation's transportation systems. The team selected eight transportation applications from the Architecture Reference for Cooperative and

Intelligent Transportation (ARC-IT) and assigned each to a group of 2-3 partner institutions from Clemson (lead), South Carolina State University (SCSU), Morgan State University (MSU), Benedict College, Florida International University (FIU), the University of Alabama at Tuscaloosa (UA), the University of Texas at Dallas (UTD), Purdue University, and the University of California, Santa Cruz (UCSC).

- In collaboration with the partner institutions, the Clemson team is developing platforms for two transportation applications, i.e., electric charging station management and integrated multimodal electronic payment, following the cybersecurity framework developed by the National Institute of Standards and Technology (NIST). Fig. 1 presents the framework developed by the Clemson researchers to perform threat modeling of a given intelligent transportation systems (ITS) application, including determination of potential strategies for attacks and the respective detection and mitigation strategies. From the national ITS reference architecture database, the team extracted detailed information related to the functional objects, processes and specifications, and data flow. This helped us replicate the application's data flow diagram (DFD) in a threat modeling tool. The team used an

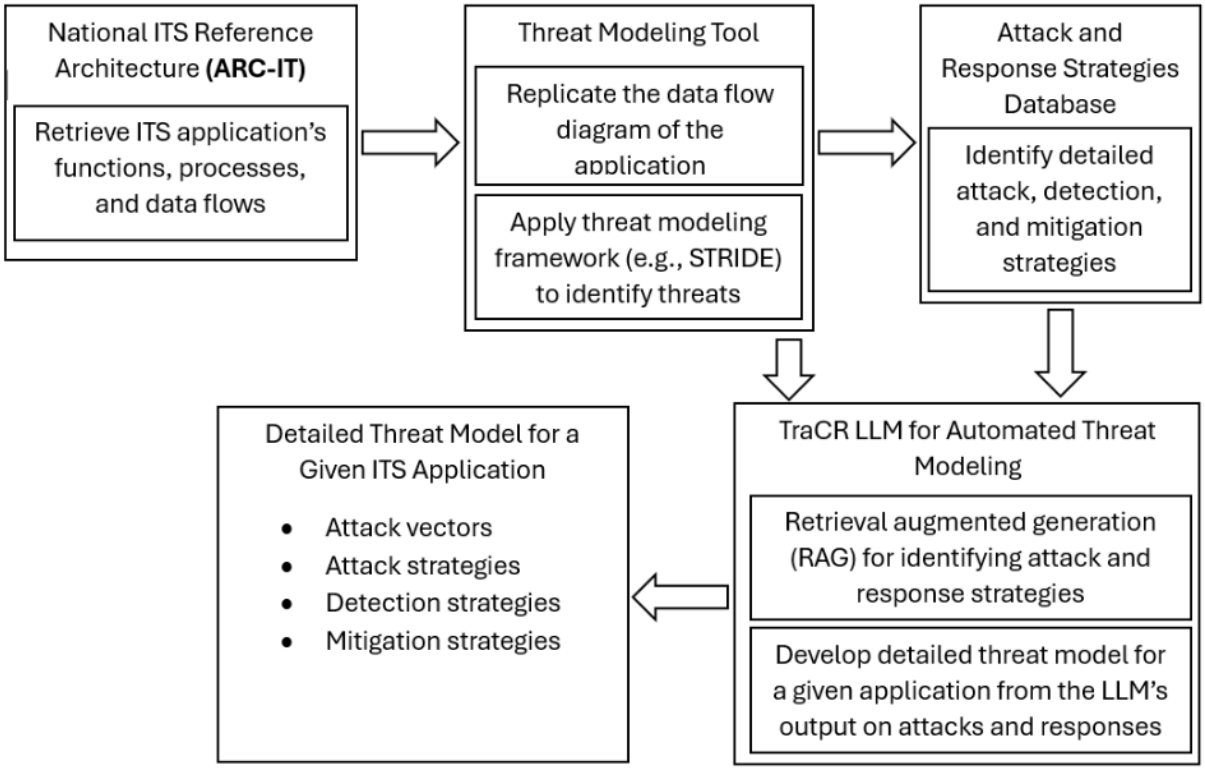

Figure 2. Threat modeling framework for a given ITS application.

open-source threat modeling tool developed by Microsoft for this purpose. Using the Microsoft threat modeling tool, the team generated a threat report following the STRIDE threat model. This report lists potential attack surfaces and corresponding attacks. The team further mapped this report to existing attack and defense databases like the MITRE ATT&CK, Common Vulnerabilities and Exposures (CVE), and Common Weakness Enumeration (CWE) databases and identified various respective attack techniques, sub-techniques, and potential detection and mitigation strategies. The TraCR team is currently working on retrieval augmented generation (RAG) using the potential threats identified by

the Microsoft threat modeling tool and the respective strategies listed on the existing database for attack, detection, and mitigation.

3) Accomplishments related to competitively selected research projects:

During Year 1, fourteen research projects were selected for funding based on external reviews from the 15 submitted proposals to an RFP sent out in Fall 2023 for competitive funding available through TraCR. Below, we feature key progress from some of the selected projects for the reporting period. The entire list of projects funded and quarterly progress reports for each project are available on the TraCR website: https://www.clemson.edu/cecas/tracr/index.html.

- **Project:** Secure and Privacy-Preserving Federated Learning for Connected and Automated Vehicles; **Lead PI:** M. Hadi Amini, FIU; **Collaborating Institutions:** MSU

  The FIU team developed hybrid privacy-preserving mechanisms to safeguard the federated learning (FL) training process and transportation user data. The team is analyzing the challenges and vulnerabilities of our systems in real-time implementation. The current version of the team's algorithm can defend against backdoor and inference attacks. As part of the inference attack defense, the team has added differential privacy to the global model by incorporating noise. The team has tested the robustness of the existing differential privacy, and based on the results, the team is developing a new local differential privacy mechanism that will be more robust and have minimal impact on the performance of the global model.

- **Project:** Cybersecurity Testbed for Connected and Autonomous Vehicles; **Lead PI:** Satish Ukkusuri, Purdue; **Collaborating Institutions:** UCSC, Benedict, MSU, Clemson

  This project aims to develop a sophisticated simulation testbed capable of assessing the multi-scale impact of cyber-attacks against connected and autonomous vehicle (CAV) fleets. To achieve this goal, the team, led by Purdue, proposed the framework with three components: a data stream, a high-fidelity virtual simulator, and a scenario generator. For the first component, the team embedded Kafka to model the data stream explicitly. The Kafka-based component can explicitly model the data stream, exposing it to potential attacks such as denial-of-service (DoS) and data spoofing. Moreover, this setup enables the separation of logic for data processing, decision generation, traffic simulation, and cyberattacks. The controller is the mediator between multiple simulation instances and the data stream. Thus, this framework guarantees strict synchronization. By broadcasting simulation ticks among the simulator, data processor, and attacker, the controller ensures consistent testing of attack algorithms. For the second component, the team developed a co-simulation tool that integrates METS-R SIM with CARLA. This framework enables the team to efficiently simulate large-scale traffic from the micro-level traffic simulation and perform photo-realistic simulations for a subnetwork using CARLA. For the third component, the team incorporated Scenic, a powerful tool for scenario generation, enabling them to create diverse and complex traffic situations. This facilitated more comprehensive testing of attack scenarios, allowing searches on a wider range of vehicle interactions for potential vulnerabilities. In the next reporting period, the team will validate the developed tool through a series of cyberattacks, including route guidance and adversarial booking attacks. The MSU team focused on developing dynamic safety margins (DSMs), which provide real-time, context-specific information to road users. Unlike Basic Safety Messages (BSMs), DSMs dynamically adapt to the environment and enhance road safety and traffic management. At MSU, significant progress was made in developing and deploying DSM capabilities using a testbed equipped with lidar technology. This testbed detects objects and conditions at intersections in real time. Lidar data is used to generate J2735 messages, broadcasted to On-Board Units (OBUs) via Roadside Units (RSUs). This system has demonstrated the ability to generate and transmit DSMs, establishing effective communication through the connected vehicle network. In parallel, a simulation-based testbed was developed to

study driver behavior under various scenarios, including cyber-attacks. A network of eight intersections has been created, and a Python function was developed to access real-time information about vehicles, including speed, throttle, brake, steering, and more. A comprehensive threat model for DSMs was developed, focusing on potential attackers, their motivations, and the types of attacks (message injection, modification, suppression, etc.). Various metrics, such as Time to Collision (TTC), were used to evaluate the potential impact of these attacks on safety and traffic disruption. A new dataset consisting of 52,000 real-world traffic sign images has been acquired to further the research on privacy-preserving FL algorithms in the context of ITS. The work on developing a hybrid privacy-preserving algorithm focuses on defending against adversarial attacks and ensuring robust and secure model training.

- **Project:** A Multi-Resolution Simulation Platform for Transportation System Security Testing and Evaluation; **Lead PI:** Yiheng Feng, Purdue; **Collaborating Institutions:** FIU
  For this project, based on the vehicle-to-everything (V2X) simulation environment, the team, led by Purdue, continued implementing attack APIs in the simulation environment. Three types of attack APIs have been added: ETA, Multi-Sensor Fusion (MSF), and route guidance attacks. *ETA attack towards infrastructure operations:* by spoofing the BSMs sent by the victim vehicle, the attacker can trigger the intersection signal controller to generate a nonoptimal signal timing plan. In the developed ETA attack API, the attacker can obtain neighboring vehicle and traffic signal states through the Simulation of Urban MObility (SUMO) interface. The neighboring vehicle states include vehicle position, speed, and acceleration. The signal controller states include elapsed green time, current signal phase, and signal plan update time. Given the neighboring vehicle and signal states, an optimization problem is formulated to generate vehicle trajectories. The generated falsified trajectories are distributed by the victim vehicle through an open source interface for running vehicular network simulations (VEINS) interface. The ETA attack API enables users to adjust attack parameters such as malicious vehicle rate. Besides, the attacker can also customize the ETA of the victim vehicle to control the attack's aggressiveness. Different ETA can impact signal control systems in various ways, leading to different outcomes in vehicle delay at intersections. In addition to customized attack parameters, the ETA attack API also enables falsified vehicle trajectories and neighboring vehicle trajectories collection. The collected trajectories can be used for analyzing and developing anomaly detection algorithms. *Multi-Sensor Fusion (MSF) attack:* In the MSF attack, the attacker compromises the MSF-based autonomous vehicle localization module and generates a falsified trajectory with lateral deviation from the ground truth trajectories. MSF attack deviates the vehicle to another lane or even the wrong direction of the roadway, potentially leading to collisions with other vehicles. A surrogate model is developed to replicate the trajectory-level attack behavior of the original MSF attack. In the attack API, the attacker obtains the victim vehicle states (i.e., vehicle position and speed) through the SUMO interface. Given the victim vehicle states, the intelligent driver model (IDM) is applied to predict the vehicle's future movement without attack. The lateral deviations for the two stages are generated according to the proposed surrogate model. The generated lateral deviation is added to the predicted future position and the attacker controls the victim vehicle to move to the spoofed position through the SUMO interface. The MSF attack API enables users to adjust attack parameters such as malicious vehicle rate. Users can also adjust traffic volume through the MSF attack API. Besides, the MSF attack API also enables the user to collect falsified vehicle trajectories and neighboring vehicle trajectories. The collected trajectories can be used to evaluate the transportation system level attack impact (i.e., crash rate). *Route guidance attack:* three main types of attacks are implemented: Route Disruption, where false information leads vehicles on suboptimal or dangerous paths; Denial of Service (DoS), which floods the system with excessive data, hindering its operation; and GPS Spoofing, where location data is falsified to misguide route decisions. Further,

API elaborates on tactics for executing these attacks, highlighting methods like falsifying traffic condition reports to misrepresent traffic jams or road closures and targeting specific times or locations during peak congestion periods. Attackers may also implement gradual changes to traffic data, which are likely to be perceived as natural fluctuations, making detection more challenging. Meanwhile, the FIU team is conducting an empirical analysis of FL attacks and simulating them on transportation simulation platforms, such as CARLA, for the multi-resolution simulation platform. The team is currently exploring the capabilities of the CARLA simulation platform. In the next reporting period, the team will integrate attack applications based on the attack APIs to evaluate their impact on the transportation system regarding safety and mobility.

- **Project:** Finding Vulnerabilities of Autonomous Vehicle Stacks to Physical Adversaries; **Lead PI:** Z. Berkay Celik, Purdue; **Collaborating Institutions:** UCSC
  This project aims to enhance the security of Automated Driving (AD) stacks against physical attacks. To this end, the team, led by Purdue, has initiated the formalization of safety properties for Autonomous Vehicles (AVs) by collecting data from NHTSA standards and driving regulations. The team is also exploring using Large Language Models (LLMs) to automate the extraction and formal representation of these properties. Concurrently, the team has been developing a language to parameterize initial conditions for scenario generation, building upon prior work on Scenic (a domain-specific probabilistic programming language for modeling the environments of cyber-physical systems). The team has adapted Scenic to specific safety properties and generated diverse scenarios. Furthermore, they have formulated the search for adversarial maneuvers as an optimization problem and explored various sampling techniques, including Reinforcement Learning and Multi-Armed Bandit Samplers. Preliminary findings highlight a trade-off between the quantity and diversity of identified adversarial maneuvers. The team has also dedicated efforts to exploring multi-agent attacks, acknowledging that adversaries could employ multiple vehicles or agents to compromise AV safety. The analysis has been broadened to generate trajectories for cooperating agents, enabling the creation of more intricate attack scenarios. In addition to these accomplishments, the team has been actively integrating their algorithms into existing falsification frameworks and investigating the potential of generative flow networks (GFlowNets) for generating diverse adversarial scenarios.
- **Project:** Hybrid Classical-quantum AI Approach for Detecting Cyberattacks in Vehicles; **Lead PI:** Shaozhi Li and Sumanta Tewari (Co-Leads), Clemson; **Collaborating Institutions:** Purdue, Benedict
  In the last reporting period, the Clemson team developed two applications that leverage quantum advantages. First, the team developed a hybrid classical-quantum deep learning library. With this library, the team designed, trained, and validated a hybrid quantum-classical convolutional neural network that outperforms classical models in distinguishing edge information within images. This enhanced capability leads to faster convergence of loss functions, significantly increasing the training speed and improving the efficiency of developing image identification systems in vehicles. Second, the team developed a deepfake attack model and the corresponding detection strategies. The deepfake attack model aims at fooling the autonomous traffic sign classification system in an autonomous vehicle into believing in fake traffic signs generated by a classical generative adversarial network (GAN). On the other hand, the deepfake detection strategy that the team developed utilizes an efficient hybrid quantum-classical neural network for deepfake detection. The hybrid approach utilizes far fewer variables and neurons when compared to classical methods, significantly reducing the size of the machine learning model. This project aims to explore the benefits of quantum computing for different problems in secure transportation. As such, the Purdue team worked on multiple avenues of improvement. First is developing quantum approaches for reinforcement learning, which have several applications in secure transportation systems. The team theoretically showed a speedup with quantum computing for average reward Markov decision processes (MDPs),

where the regret in classical computing is O(sqrt(T)), while quantum computing achieves the regret of O(log(T)). This shows an exponential regret improvement, demonstrating the quantum supremacy. In the second study, the team proposed a hybrid quantum-classical scalable non-local neural network, Quantum Non-Local Neural Network (QNL-Net), to enhance pattern recognition. The proposed QNL-Net relies on inherent quantum parallelism to allow the simultaneous processing of many input features, enabling more efficient computations in quantum-enhanced feature space and involving pairwise relationships through quantum entanglement. The approach was benchmarked on multiple vision datasets and can improve the classification in transportation security datasets. In the third study (ongoing), the team formulated the vehicle routing problem with edge interdictors as a mixed integer linear program. The team is working on the quantum supremacy of the resilience of the problem using quantum annealing approaches.

- **Project:** Multimodal In-Vehicle Sensor Fusion for Cyber-Secured Autonomous Navigation; **Lead PI:** Mizanur Rahman, UA; **Collaborating Institutions:** Clemson
  For this project, the UA team has developed a cyber-resilient navigation system for autonomous vehicles. This development is an extension of an NSF-funded project. The resilient navigation system can detect spoofing attacks on Global Positioning System (GPS)-based navigation systems and can guide an autonomous vehicle to its destination without GPS assistance, relying solely on in-vehicle sensors such as accelerometers, gyroscopes, and cameras, aided by low-cost map. This system was demonstrated at the TraCR Annual Conference 2024 in Greenville, SC, on May 5-6, 2024, and at the USDOT Future of Transportation (FoT) Summit 2024 in Washington, DC, on August 15-19, 2024. Moreover, the UA and Clemson teams are collaborating on a review paper on autonomous vehicle navigation cybersecurity, which is nearing completion. CU is leading the development of a trustworthy solution for integrated navigation systems for autonomous vehicles.

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, 3) conference sessions, and 4) 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 includes:
  - Dr. Paul Wang, Professor and Chair, Morgan State University, **Advances in Quantum Cryptography and Next Generation Quantum Internet** (April 2024)
  - Dr. Mizanur Rahman, Assistant Professor, The University of Alabama, Tuscaloosa, **Cyber Resilient GNSS-based Navigation for Autonomous Ground Vehicles under Threat Uncertainties and Contested Urban Environments** (August 2024).
  - Dr. Z. Berkay Celik, Assistant Professor Purdue University, **Towards Compositional Secure Autonomy: From Perception to Control** (October 2024).
- Dr. Satish Ukkusuri (Purdue) hosted Dr. Patricia Mokhtarian, School of Civil and Environmental Engineering at the Georgia Institute of Technology, for a seminar at Purdue in September 2024.

2) Workshops

- Dr. Mizanur Rahman (UA) presented the cybersecurity aspect of transportation systems in a workshop arranged by Dr. Hope Drummonds-Whiteside of the Alabama Transportation Institute for STEM high school teachers at UA on June 15th, 2024.
- MSU organized a summer camp for high school and middle school students, introducing them to cybersecurity challenges in the transportation sector. Students explored various cyberattacks, their

potential impacts on transportation systems, and measures to protect against them. They also learned about the unique cybersecurity challenges in Connected and Autonomous Vehicles (CAVs) and the technologies used to protect these systems from hacking and other threats.

- Dr. Daniel Fremont (UCSC) organized a workshop at the UCSC campus for the open-source Scenic Language that he developed (Scenic is a tool used to test the security and safety of autonomous vehicles). More information about the workshop is available at: https://scenic-lang.org/workshop24/. The participants included over 30 developers and potential users of this framework.
- Dr. Daniel Fremont also co-organized a tutorial on the Scenic language at the CVPR 2024 conference on June 17th, 2024. More information about the tutorial is available at: https://cvpr.thecvf.com/virtual/2024/tutorial/23734.
- Dr. Cihang Xie (UCSC) co-organized the 4th Workshop of Adversarial Machine Learning on Computer Vision: Robustness of Foundation Models at CVPR 2024.
- Dr. Cihang Xie also co-organized the Out of Distribution Generalization in Computer Vision Workshop at ECCV 2024.
- Dr. Leilani Gilpin (UCSC) and her student Oliver Chang co-organized the XAI for Deep Reinforcement Learning workshop at AAAI 2024. More information about the workshop is available at: https://xai4drl.github.io/. The workshop included several results on autonomous vehicles.
- On May 4th, 2024, TraCR participated in the Habitat Tech Fair organized by Habitat for Humanity of Greenville County. This event aimed at engaging members of traditionally underserved communities. Dr. Ronnie Chowdhury and members of the Clemson University (Clemson) team delivered presentations to young students and their parents, showcasing the opportunities in technology and cybersecurity. They emphasized the rewarding career paths in the field and outlined the qualifications and skills required to enter it. The primary goal was to inform and inspire, and in particular, to highlight how high-paying jobs in cybersecurity could empower families to afford homes and resist the pressures of gentrification in their neighborhoods.
- TraCR participated in the Benedict College Cybersecurity and E-sport summer event, where Dr. Ronnie Chowdhury led a presentation session. He informed the attendees about cybersecurity and emphasized the critical role quantum computing will play in the future of technology. Additionally, a technology demonstration provided the students with hands-on experience, offering them a glimpse into the cutting-edge advances shaping the future of cybersecurity.
- During the summer of 2024, TraCR hosted two cybersecurity workshops specifically for underrepresented students from middle school through high school through Benedict College Summer Transportation Institute (STI). The programs introduced the students to the foundations of cybersecurity and sought to bridge the gap in cybersecurity education for underrepresented groups. The workshops offered hands-on experience and practical knowledge in this increasingly vital field. Through interactive sessions and real-world scenarios, students were introduced to key concepts such as network security, ethical hacking, data protection, and hardware security. The workshops also underscored the importance of cybersecurity in everyday life, encouraging students to consider careers in this dynamic and growing field.
- On July 12th, 2024, Dr. Ronnie Chowdhury gave a talk to the City of Greenville summer camp's students called “STEM: the Path to Exciting Careers in New Frontiers.” He encouraged the students to explore careers in science, technology, engineering, and math, showing them how these fields offer exciting opportunities. The Clemson team also ran a fun and interactive workshop on cybersecurity, where they taught the campers about real-world threats and the importance of securing digital information.
- Dr. M Sabbir Salek and Ms. Megha Patel (both from Clemson) attended the CUTC Summer Meeting in South Padre Island, TX, from June 10-12, 2024.

- Dr. Ronnie Chowdhury conducted a career workshop for engineering students from Claflin University at Orangeburg, SC, on Sep 18th, 2024. The title of his workshop was "Opportunities for Careers and Capacity Building in the Emerging Quantum Information Science."

3) Conference sessions

- TraCR led a session highlighting careers in quantum information systems at The Men of Color National Summit organized by Clemson University. The summit aims to narrow the educational disparity among African American and Hispanic males in colleges. The summit is a nationwide platform for students and professionals to convene, engage with expert speakers, and motivate one another. This year's event on April 11th, 2024, at the Greenville Convention Center in Greenville, SC, marked the seventh iteration of the summit. The summit drew over 2,000 attendees, including high school and college students, business professionals, educators, government officials, and industry leaders.
- TraCR organized a session entitled "Cybersecurity: Threats and Opportunities" at the annual SC EPSCoR State Conference on April 9th, 2024, in Columbia, SC. The primary objective of the conference is to unite South Carolina faculty, postdoctoral fellows, graduate and undergraduate students, and STEM professionals, fostering networking and encouraging collaborative efforts. The session organized by TraCR and moderated by Dr. Ronnie Chowdhury harmonized seamlessly with the TraCR's mission by featuring talks from Dr. Zhenkai Zhang (Clemson), Mr. Rick Siebenaler (Maritime Cybersecurity Institute), and Mr. Leon Geter (Benedict College).
- Jean Michel Tine, MSI coordinator, was a panelist in the Pathways to Entrepreneurship Pilot Experience on September 10th, 2024, at USDOT headquarters in Washington, DC. The summit supports the USDOT's mission to foster opportunities for small and disadvantaged businesses. He shared his career journey with participants, hoping to create an impact as they begin their entrepreneurial endeavors.
- Dr. Alvaro Cardenas (UCSU) served as a co-chair for the 19th ACM Asia Conference on Computer and Communications Security (ASIACCS) 2024.
- Dr. Alvaro Cardenas also served as a co-chair for the NSF 2024 Secure and Trustworthy Cyberspace Principal Investigator's Meeting.
- Dr. Alvaro Cardenas also participated in the steering committee of two conferences focused on the security of cyber-physical systems and smart vehicles: (i) ACM Cyber-Physical Systems and Internet of Things Security and Privacy Workshop 2024 (CPSIoTSec), and (ii) EAI International Conference on Security and Privacy in Cyber-Physical Systems and Smart Vehicles 2024 (SmartSP).

4) Courses

- The UTD team introduced a unit on Integrating AI and Cyber Security for Transportation Systems in the course *Data and Applications Security and Privacy* during the Spring semester of 2024.
- The UTD team also introduced a course in *Generative AI and Large Language Models* in which security issues are discussed in one unit.
- The Clemson team is currently developing a new e-learning module called the *Zero Trust Model*. This module is designed to provide a comprehensive introduction to the Zero Trust security framework, covering its fundamental principles, key components, and real-world applications. By completing this module, participants will understand how to implement Zero Trust strategies to mitigate cybersecurity risks in network infrastructures and Connected and Autonomous Vehicles (CAVs).

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 disseminate several results and outcomes. The website includes a list and abstract of all competitively selected projects,

quarterly reports from each selected project, and the center's quarterly newsletter. In addition, we continue to use our several social media outlets to disseminate key information about the center (links below).
  - LinkedIn: http://www.linkedin.com/company/tracr-usdot-utc
  - Twitter: https://twitter.com/TraCR_UTC
  - YouTube: https://www.youtube.com/@TraCR-UTC
- A total of 10 publications (published/accepted) in books and journals and 27 conference papers and/or presentations were contributed by TraCR-affiliated faculty members and students during the reporting period of April 1st, 2024, to September 30th, 2024, to disseminate the results obtained. A detailed list of these is provided below in the report in the section on Outputs.
- TraCR researchers also delivered several keynote/invited presentations to disseminate research results. A list of these keynote talks is given below:
  - Dr. Mizanur Rahman delivered an invited talk titled "Cybersecure GNSS-Based Navigation for Autonomous Ground Vehicles" at the 2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2024) in Knoxville, TN, USA, from July 1-3, 2024. His presentation addressed the challenges of securing GNSS-based navigation systems against cyber threats and proposed innovative solutions to enhance cybersecurity in autonomous ground vehicles.
  - Dr. Mizanur Rahman attended the 6th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting on September 4-5, 2024, in Pittsburgh, Pennsylvania, and presented on "Cyber Resilient Navigation for Autonomous Systems under Threat Uncertainties and Contested Environments."
  - Dr. Mansoureh Jeihani (MSU) presented work on the Scott Key bridge collapse, focusing on modern transportation systems' technological and safety challenges.
  - Dr. Alvaro Cardenas was the keynote speaker for the 10th ACM Cyber-Physical Systems Security Workshop (CPSS) 2024.
  - Dr. Alvaro Cardenas was also a keynote speaker at the Silicon Valley Cybersecurity Conference (SVCC) 2024.
  - Dr. Bhavani Thuraisingham (UTD) delivered a keynote presentation at the ACM SACMAT Conference (a top-tier data and applications security conference) on AI for Transportation Systems Security.
- In addition to the publications and conference presentations, several live technology demonstrations were conducted by TraCR researchers based on results obtained during the reporting period. A list of these live technology demonstrations and the venue is provided below:
  - The Clemson team demonstrated two technologies at the FoT Summit 2024: 1) Hardware Security Attacks and Their Detection, and 2) Quantum Supremacy for Transportation Cybersecurity.
  - The Clemson team demonstrated five technologies at the TraCR Annual Conference 2024: 1) Secure Real-time Collision Warning Application Using Heterogeneous Wireless Networking, 2) Vision-Based Pedestrian Safety Alert System, 3) Vision-based Basic Safety Message Generation and Collision Warning System, 4) Hardware Security Attacks and Their Detection, and 5) Quantum Supremacy.
  - Dr. Mizanur Rahman and his research team from UA conducted a live demonstration of cyber-resilient navigation technologies for autonomous vehicles at the TraCR Annual Conference 2024, Greenville, SC, May 5-6, 2024.
  - Dr. Mizanur Rahman and his research team from UA conducted a live demonstration of cyber-resilient navigation technologies for autonomous vehicles at the USDOT Future of Transportation

Summit 2024, Washington, DC, August 15-19, 2024.
- The MSU team showcased advanced technology related to Connected and Autonomous Vehicles (CAVs), AI systems for road user detection, and the autonomous wheelchair that can transport passengers in airports.
- The UTD team conducted a demonstration of 'RAG-driven LLM' to identify loopholes in legal landscape at the TraCR Annual Conference 2024, Greenville, SC, May 5-6, 2024.
- Dr. Latifur Khan and his research team at UA conducted a live demonstration of TraCR AI - a large language model trained on current cybersecurity legislation across the U.S. at the TraCR Annual Conference 2024, Greenville, SC, May 5-6, 2024.

1.5. **What do you plan to do during the next reporting period to accomplish the goals and objectives?**
For the next reporting period, our goals and objectives 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 scheduled distinguished speaker for November 2024 is Dr. Kemal Akkaya from Florida International University. His webinar topic will be "Leveraging Generative AI for Sensor Data Falsification on Drones and Automated Vehicles".
- Jean Michel Tine (from Clemson) will lead a workshop at Benedict College on October 9th, 2024. The participants will be introduced to a hands-on session on Pytorch and will understand how the library works and how to load, preprocess data, and then build and evaluate a Convolution Neural Network.
- Sefatun Noor-Puspa (from Clemson) will lead a workshop at Benedict College on October 9th, 2024, on Introduction to Hardware Implementation on FPGA Board Using Vivado. In this module, students will be introduced to the fundamental concepts of digital circuit design, starting with basic logic circuits.
- Dr. Ronnie Chowdhury will be the distinguished webinar speaker at Morgan State University on November 12th, 2024. The talk will be on Cybersecurity and the goal is to inform and impact the students in the evolving area of Cybersecurity.
- Dr. Ronnie Chowdhury will attend the International Alliance for Mobility Testing and Standardization (IAMTS) General Assembly on Oct 14th, 2024, as the lead for their cybersecurity thrust.
- Dr. Ronnie Chowdhury will be 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 will be part of the panel discussion where the experts will discuss 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 Tine will visit Claflin University on October 17th, 2024, for the Graduate and Professional School Visitation Day to talk about careers in cybersecurity.
- Dr. Ronnie Chowdhury will be part of the CYBER-CARE Symposium, where he will be part of the keynote panel 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 will be the distinguished webinar speaker for the Computer Science department at FIU on October 18th, 2024, and will talk on Cyber-Physical-Social Systems and Its Security and Resiliency.
- Dr. Z. Berkay Celik will serve as the general chair of the Symposium on Vehicle Security and Privacy

(VehicleSec) 2025. VehicleSec will take place on August 11-12, 2025 at the Seattle Convention Center in Seattle, WA, USA, and will be co-located with the esteemed USENIX Security Symposium.

- Dr. Mizanur Rahman will attend the West Alabama Works (WOW) event for K-12 students at the Shelton State Community College, Tuscaloosa, AL, to inspire students to choose their careers in transportation engineering focusing on cybersecurity.
- Dr. Bhavani Thuraisingham plans to present UTD's work from TraCR projects at several universities while on sabbatical for 2024-2025. Currently presentations are planned at NJIT, UCI, and USC.
- Dr. Hadi Amini (FIU) will present on Simple Analytical Models For Estimating the Queue Lengths from Probe Vehicles at Traffic Signals II: A Combinatorial Approach for Nonparametric Models on October 26th, 2024.
- Dr. Alvaro Cardenas will be a keynote speaker at the 6th Joint Workshop on CPS & IoT Security and Privacy.
- A cyber competition team from MSU will participate in the Spectral Cloak National Cyber Competition on October 26th, 2024. This competition is sponsored by the National Security Engineering Center, a Federally Funded Research and Development Center managed by MITRE competition. Dr. Amjad Ali, a co-PI at MSU, is the lead mentor to the MSU cyber competition team members. The purpose of this competition is to inspire students to pursue cybersecurity careers by introducing them to cyberspace attacks and defense using a fully featured exploitation framework in a scenario-driven environment.

2) Plans for foundational project:

Clemson researchers involved in the foundational project will continue with their ongoing effort to develop a platform for automated threat modeling. The team will focus on two to three ITS applications as case studies and conduct detailed threat modeling utilizing a large language model (LLM)-based approach that utilizes retrieval augmented generation (RAG) using existing database on attacks, and detection and mitigation strategies. The threat modeling report generated from the output of the LLM will be validated with security experts. In addition, we will focus on automating the threat modeling framework (presented in Fig. 1) over the next reporting period. In addition, the team is focusing on connected vehicle traffic signal systems application for the foundation project. The team will simulate Cellular Vehicle-to-Everything (C-V2X) communication between road users and roadside units (RSUs) to assess and enhance the cybersecurity resilience of vehicular communication systems for the foundational project. By implementing the IEEE 1609 family of standards, known collectively as Wireless Access in Vehicular Environments (WAVE), our simulation will adhere to industry protocols for secure vehicular communications. The simulation will also incorporate NIST guidelines relevant to cybersecurity frameworks in ITS. Various attack scenarios—including denial-of-service (DoS), man-in-the-middle (MitM), spoofing, and replay attacks—will be tested on current standard C-V2X communication protocols to evaluate their impact on system performance and safety. This comprehensive approach aims to identify vulnerabilities in existing protocols and develop mitigation strategies that enhance the resilience of C-V2X communications against cyber threats, thereby contributing to the advancement of secure ITS infrastructures.

3) Plans for competitively-selected projects:

The TraCR board of directors will meet between early- and mid-November to discuss the research proposals received through the RFP for year 2 competitively selected proposals and reviews from external reviewers to decide which competitive projects to support during the current fiscal year. The funding recipients will be notified shortly after the meeting. Selected research proposals will be funded through TraCR to begin research activities in January 2025.

2. PARTICIPANTS & COLLABORATING ORGANIZATIONS:

TraCR is a diverse, experienced, and geographically distributed consortium of nine partners:

- Clemson University (Clemson)
- Benedict College (Benedict)
- Florida International University (FIU)
- Morgan State University (MSU)
- Purdue University (Purdue)
- South Carolina State University (SCSU)
- The University of Alabama at Tuscaloosa (UA)
- The University of California, Santa Cruz (UCSC)
- The University of Texas at Dallas (UTD)

We have established the following collaborations during Year 1:

Clemson is collaborating with:

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

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, will contribute to TraCR research on GNSS-based cyber-resilient navigation for autonomous systems.
- Spirent Federal Systems Inc. provided Spirent GSS9000, which is a hardware-in-the-loop Global Navigation Satellite Systems (GNSS) simulator package and is pivotal for enhancing the university's cyber-resilient Position, Navigation, and Timing (PNT) research facilities, as well as bolstering PNT-related educational programs and workforce development initiatives.

MSU is collaborating with:

Maryland Transit, which is sharing its knowledge of current, state-of-the-art transit security management.

Purdue is collaborating with:

Qualcomm (Dr. Jonathan Petit and Mr. Raashid Ansari) on implementing the VASP platform for the competitively selected project A Multi-Resolution Simulation Platform for Transportation System Security Testing and Evaluation.

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

1. Abdeen, B., Al-Shaer, E., Singhal, A., Khan, L., and Hamlen, K. 2024. SMET: Semantic Mapping of CTI reports and CVE to ATT&CK for Advanced Threat Intelligence. *Journal of Computer Security*, in press
2. Comert, G., Amdeberhan, T., Begashaw, N., Medhin, N., Chowdhury, M., 2024. Simple analytical models for estimating the queue lengths from probe vehicles at traffic signals: a combinatorial

approach for nonparametric models. *Expert Systems with Applications*, 252, 124076.
3. Desai, H., and Kantarcioglu, M., Chapter 14: Blockchains and intelligent transportation system applications. In: *Data Analytics for Intelligent Transportation Systems*, 2nd Edition, Elsevier, in press.
4. Dasgupta, S., Irfan, M.S., Rahman, M. and Chowdhury, M., 2024. Chapter 15: Modeling, detection, and mitigation of global navigation satellite system spoofing attack in ground transportation systems. In: *Data Analytics for Intelligent Transportation Systems*, 2nd Edition, Elsevier, in press.
5. Mia, J., Amini, M. H., 2024. A Secure Object Detection Technique for Intelligent Transportation Systems. *IEEE Open Journal of Intelligent Transportation Systems*, 5, 495-508.
6. Saha, N., Rezapour, S., Sahin, N. C., Amini, M. H., 2024. Coordinated Restoration of Interdependent Critical Infrastructures: A Novel Distributed Decision-Making Mechanism Integrating Optimization and Reinforcement Learning. *Sustainable Cities and Societies*, 114, 105761.
7. Ganguly, B., Xu, Y., Aggarwal. V., 2024. Quantum Acceleration of Infinite Horizon Average-Reward Reinforcement Learning. arXiv:2310.11684
8. Gupta, S., Konar, D., Aggarwal, V., 2024. A Scalable Quantum Non-local Neural Network for Image Classification. arXiv:2407.18906
9. Zhu, R-J., Wang, Z., Gilpin, L., Eshraghian, J.K. 2024. Autonomous Driving with Spiking Neural Networks. arXiv:2405.19687.
10. Hockstad, T., Rahman, M., Jones, S., Chowdhury, M., 2024. A Regulatory Gap Analysis in Transportation Cybersecurity and Data Privacy. *Transportation*, accepted.
11. Thai, M. T., Phan, H. N., Thuraisingham, B, 2025. Handbook of Trustworthy Federated Learning. Springer Cham, ISBN 978-3-031-58922-5.
12. Thuraisingham, B., 2025. Trustworthy Machine Learning. CRC Press, in press.
13. Li, S., Salek, M.S., Wang, Y., Chowdhury, M., 2024. Quantum-inspired activation functions and quantum Chebyshev-polynomial network. *IEEE Transactions on Neural Networks and Learning Systems*, under review.
14. Rahman, M., Islam, M., Deka, L. and Chowdhury, M., 2024. Introduction to Special Issue on Cybersecurity and Resiliency for Transportation Cyber-Physical Systems. Journal on Autonomous Transportation Systems, 1(4), pp.1-3.
15. Shakib, K.H., Rahman, M., Islam, M., and Chowdhury, M., 2024. Quantum Shor's Algorithm-based Impersonation Attack on Blockchain-based Vehicular Ad-hoc Network. IEEE Transactions on Intelligent Transportation Systems, under review.
16. Ameen Noman, S., Atkison, T., Sami Irfan, M., and Rahman, M., 2024. A Predictive Approach for Sybil Attack Detection for a Waiting Time-Based Adaptive Traffic Signal Controller. ACM Journal on Autonomous Transportation Systems, under revision.

2) Conference Papers/Presentations

1. Tine, J.-M. The Ethical Integration of Artificial Intelligence in Civil Engineering. Presented at the 2024 ASCE Symposium, Charlotte, NC, April 2024.
2. Tine, J.-M., Comert, G., Chowdhury, M. Efficacy of Statistical, Long Short-Term Memory (LSTM), and Quantum LSTM in Cyber-Attack Detection for Connected Vehicles. Presented at the 2024 SC EPSCoR Conference, Columbia, SC, April 2024.
3. Salek, M. S., Mamun, A. A., Chowdhury, M. Adversarial Attack-Resilient Traffic Sign Classification System for Autonomous Vehicles. Presented at the 2024 SC EPSCoR Conference, Columbia, SC, April 2024.
4. Rahman, A., Tine, J.-M., Salek, M.S., Chowdhury, M. AI-Supported Heterogeneous Wireless Networking for Efficient and Secure Connected Vehicle Applications in Rural Areas TraCR Annual Conference, Greenville, SC, May 06, 2024.

5. Enan, A. and Chowdhury, M. Stealthy Attacker Among Us: Problem and Solution. TraCR Annual Conference, Greenville, SC, May 06, 2024.
6. Salek, M.S., Mamun, A.A., Chowdhury, M. AR-GAN: Generative Adversarial Network-Based Defense Method Against Adversarial Attacks on the Traffic Sign Classification System of Autonomous Vehicles. TraCR Annual Conference, Greenville, SC, May 06, 2024.
7. Thomas, O., Tine, J.-M., Salek, M.S., and Chowdhury, M. Transportation Cybersecurity Vulnerabilities, Failures, and Improvement Strategies. TraCR Annual Conference, Greenville, SC, May 06, 2024.
8. Majumder, R., Munnings, T., Stubbs, A., Tadessa, N., Werth, D., Gale, A., Mbamalu, G., Comert, G., Salek, M., Chowdhury, M. Graphs-powered Secured Surveillance: Drones Detecting Methane, Fortified Against Cyber Threats. C2M2 8th Annual Conference, Columbia, SC, August 22, 2024.
9. Tine, J.-M., Comert, G., and Chowdhury, M. Efficacy of Bayesian Online Changepoint Detection, Long Short-Term Memory, and Quantum Long Short-Term Memory for Real-Time Cyber-Attack Detection in a Connected Vehicle Environment. TraCR Annual Conference, Greenville, SC, May 06, 2024.
10. Puspa, S. N., Chowdhury, M. Hardware Trojan in Transportation. Presented at the 2024 SC EPSCoR Conference, Columbia, SC, April 2024.
11. Zhang, L., Burbano, L., Chen, X., Cardenas, A. A., Drager, S., Adderson, M., and Kong, F. Fast Attack Recovery for Stochastic Cyber-Physical Systems. IEEE Real-Time and Embedded Technology and Applications Symposium, Hong Kong, China, May 2024.
12. Hockstad, T., Akbar, K., Uddin, M. A Regulatory Gap Analysis in Transportation Cybersecurity and Data Privacy. Presented at the TraCR Annual Conference, Greenville, SC, May 2024.
13. Akbar, K., Uddin, M., Khan, L. Bridging Legal Knowledge Gaps in Cybersecurity for Connected and Automated Transportation Systems with Large Language Models. Presented at the TraCR Annual Conference, Greenville, SC, May 2024.
14. Hasan, K.H., Rahman, M., Islam, M., Chowdhury, M. Impersonation attack modeling for a blockchain-based vehicular ad-hoc network using quantum Shor's algorithm. Presented at the TraCR Annual Conference, Greenville, SC, May 2024.
15. Dasgupta, S., Ahmed, A., Irfan, S.M., Rahman, M., Bandi, T. Unveiling the stealthy threat: Analyzing slow drift GPS spoofing attacks for autonomous vehicles in urban environments and enabling the resilience. Presented at the TraCR Annual Conference, Greenville, SC, May 2024.
16. Dasgupta, S., Shakib, K.H., Irfan, S.M., Rahman, M. Experimental validation of sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles. Presented at the TraCR Annual Conference, Greenville, SC, May 2024.
17. Aldeen, M., MohajerAnsari, P., Ma, J., Chowdhury, M., Cheng, L., Pése, M.D. An Initial Exploration of Employing Large Multimodal Models in Defending Against Autonomous Vehicles Attacks. Presented at the 2024 IEEE Intelligent Vehicles Symposium (IV), Jeju Island, Korea, June 2024.
18. Aldeen, M., MohajerAnsari, P., Ma, J., Chowdhury, M. A., Cheng, L., Pesé, M. D., 2024. A First Look at Employing Large Multimodal Models Against Autonomous Vehicle Attacks. ISOC Symposium on Vehicle Security and Privacy (VehicleSec '24).
19. Ding, W., Liao, S., Cheng, L., Mi, X., Zhao, Z., Hu. H, Command Hijacking on Voice-Controlled IoT in Amazon Alexa Platform. Presented at the 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24), Singapore, July 2024.
20. Mia, J., Amini, M. H. An Empirical Analysis of Secure Federated Learning for Autonomous Vehicle Applications. Presented at ASCE International Conference on Computing in Civil Engineering, Carnegie Mellon University, Pittsburgh, PA, July 2024.
21. Sweeting, D., Iyangar, B., Comert, G., Begashaw N. Traffic Incident Detection Using Sumo Simulation With TracII Interface. Presented at Summer Undergraduate Research Institute, Benedict College, Columbia SC, July 2024.

22. Hockstad, T., Rahman, M., Jones, S., Chowdhury, M., Khan, L. Resolving Legislative Gaps in Transportation Cybersecurity Policy. Presented at the Future of Transportation Summit, Washington, DC, August 2024.
23. Chang, O., Kamat, A.A., Self, W. Collaborative Embodied Reasoning in Autonomous Driving. Presented at the Workshop on Training Agents with Foundation Models at RLC 2024, Amherst, MA, August 2024.
24. Dasgupta, S., Ahmed, A., Irfan, S.M., Rahman, M., Bandi, T. Irfan, M.S. Unveiling the Stealthy Threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling Resilience. Presented at the Alabama Collaborative for Contemporary Education in Precision Timing (ACCEPT) Annual Meeting and Workshop, Tuscaloosa, AL, August 2024.
25. Dasgupta, S., Shakib, K.H., Irfan, S.M., Rahman, M. Experimental Validation of Sensor Fusion-Based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. Presented at the Alabama Collaborative for Contemporary Education in Precision Timing (ACCEPT) Annual Meeting and Workshop, Tuscaloosa, AL, August 2024.
26. Pinder, S., Iyangar, B., Comert, G., Gale, A., Chowdhury, M. Preparation of Graphical User-Interface in Real-Time for Low-Cost Methane Detection Sensors using Shiny. Presented at the EM MSIPP Achievement Awards Workshop, Augusta, GA, August 2024.
27. Godoy, H., Comert, G., Gale, A., Rolle, C. Low-Cost Methane Sensor Development and Deployment at Solid Waste Facilities. Presented at the EM MSIPP Achievement Awards Workshop, Augusta, GA, August 2024.

3) ***Theses and Dissertations***

1. Raza Ahmer (B.S., Computer Science, Clemson), “carroot: A Secure Automotive ECU for Connected Vehicles.”
2. Muhammad Sami Irfan (M.S., Civil Engineering, UA), “Transportation digital twin framework and its vulnerabilities against cyber-attacks.”
3. Kazi Shakib (M.S., Civil Engineering, UA), “Small-key based post-quantum cryptographic scheme for blockchain-based vehicular ad-hoc network (Vanet).”
4. Abyad Enan (M.S., Civil Engineering, Clemson), “Basic Safety message generation through video-based analytics for potential safety applications.”
5. Namrata Saha (Ph.D., Computer Science, FIU), “Coupled reinforcement learning for resilient interdependent networks.”
6. Sagar Dasgupta (Ph.D., Civil Engineering, UA), “Security of GNSS-based navigation systems in autonomous vehicles.”
7. Xiaowei Chen (Ph.D., Civil Engineering, Purdue), “Advancing operational algorithms for electric mobility systems modeling.”
8. Okpala Ebuka Johnbosco (Ph.D., Computer Science, Clemson), “Offensive content detection on online social platforms.”

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

- The official website of TraCR is available at https://www.clemson.edu/cecas/tracr/. The website was launched in October 2023 and details the center’s activities. The Research tab on the website provides details about the various thrusts for the center, while all Request for Proposals (RFPs) for competitive funding every year will also be posted here. We have already posted the first RFP on the TraCR website, a list of projects selected through the RFP, and their abstract. Highlights from our outreach activities targeted towards under-represented students are posted under the Diversity Initiatives tab. We have also included our data management plan and all center reports so far, and we plan on posting progress and general reports from competitive projects selected every year.

- The Twitter/X page for TraCR was launched in September 2023 and is available at https://twitter.com/TraCR_UTC. This social media page was expanded with user engagement and aims to provide updates related to the center's activities – including announcements for webinars and the latest news from the center – to those in the broader transportation community.
- The YouTube channel for TraCR is available at https://www.youtube.com/@TraCR-UTC. We will continue to share recordings of all TraCR Scholar Webinar series on the channel. To date, we have uploaded all webinars to the channel. We will also share all videos related to the center through this YouTube channel.
- The LinkedIn page for TraCR is available at http://www.linkedin.com/company/tracr-usdot-utc. The LinkedIn page serves as a place to reach out to the professional community with the latest on TraCR's activities. This will also be the portal where we post all job openings related to TraCR to reach a wide range of potential applicants.

3.2. **Technologies or techniques**

Based on the virtual simulation testbed developed in the competitively funded project "Cybersecurity Testbed for Connected and Autonomous Vehicles" the Purdue team has created a physical testbed consisting of several miniature vehicles equipped with a variety of sensors (time-of-flight (ToF) sensors, cameras, and inertial measurement units (IMUs)) along with several smart roadside traffic lights to simulate real-world traffic scenarios. In this expanded setup, the cyberattacks studied in the project will be transferred to a physical environment along with simulation maps.

3.3. **Inventions, patent applications, and/or licenses**

Nothing to report yet.

4. **OUTCOMES:**

- The hybrid privacy-preserving algorithm developed at FIU enhances the security of federated learning in ITS by defending against malicious attacks, specifically in object detection tasks. This algorithm enables autonomous vehicles and roadside units to collaboratively train models while maintaining data privacy, providing robust protection against data poisoning-based model replacement and inference attacks. The development of a novel hybrid privacy-preserving algorithm by the FIU team enhances the security of ITS, particularly by defending against malicious attacks during federated learning training and inference phases. By safeguarding object recognition tasks within machine learning applications, this project significantly improves transportation safety, reliability, and system resilience against cyber threats.
- The Clemson team developed a hybrid classical-quantum deep learning library. With this library, anyone can design and train quantum convolutional neural networks (CNNs) that can extract distinguishing edge information in images more efficiently that classical CNNs. The team also developed a deepfake attack model that could fool the traffic sign detection system in an autonomous vehicle by injecting fake images.
- The method, CorBin-FL, developed at FIU, significantly advances privacy-preserving techniques in federated learning by enhancing privacy without compromising model accuracy. This method, along with its extension AugCorBin-FL, improves the practicality of federated learning in sensitive applications by optimizing the privacy-utility trade-off. Additionally, CorBin-FL sets a new benchmark in differential privacy for distributed machine learning, outperforming traditional Gaussian and Laplacian methods.
- The dynamic safety margin (DSM) threat model developed at MSU for enhanced cybersecurity for connected vehicles has helped identify and mitigate vulnerabilities in-vehicle communication,

increasing safety at intersections and improving traffic flow resilience.

5. **IMPACTS:**

TraCR was established last year, and this is our third reporting period for the semi-annual progress report. Our activities have had several impacts already, highlighted below, and we expect to see a continuing significant impact soon as the TraCR-supported competitively selected research projects are wrapped up at the end of the calendar year and new projects are selected for Year 2.

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

- The Habitat for Humanity of Greenville County (HFHGC) was awarded a $10,000 grant from the Hubble Foundation to support the launch of technology centers, in collaboration with TraCR, in marginalized communities of color. The first center will open in January 2025 at the Sterling Hope Center in the Sterling Community. This partnership between TraCR and HFHGC represents a shared vision of fostering economic development, reducing inequality, and creating sustainable, thriving communities. Specifically, TraCR will (1) provide faculty and student volunteers to support educational programs and mentorship; (2) support developing and delivering curricula focused on technology skills, entrepreneurship, and digital literacy; and (3) support research and data collection to measure the program's impact on participants and the broader community.
- The Clemson team has made a significant impact on the seniors of Benedict College by providing targeted workshops in Deep Learning and Hardware Synthesis and mentoring support within the CSC 430 Senior Research and Professional Experience course. Clemson's hands-on approach introduced the 15 enrolled students to practical aspects of cybersecurity and cutting-edge research.

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?**

Nothing to report yet.

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**

For Benedict College, Associate Director Dr. Gurcan Comert has moved to North Carolina A&T University. The new Associate Director of TraCR at Benedict College will be Dr. Balaji Iyangar. During the reporting period, we have worked with Dr. Iyangar to bring him up to speed.

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.