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: April 30, 2024
DUNS#: 0426298
EIN#: 57-6000254

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

Signature of Submitting Official:

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.

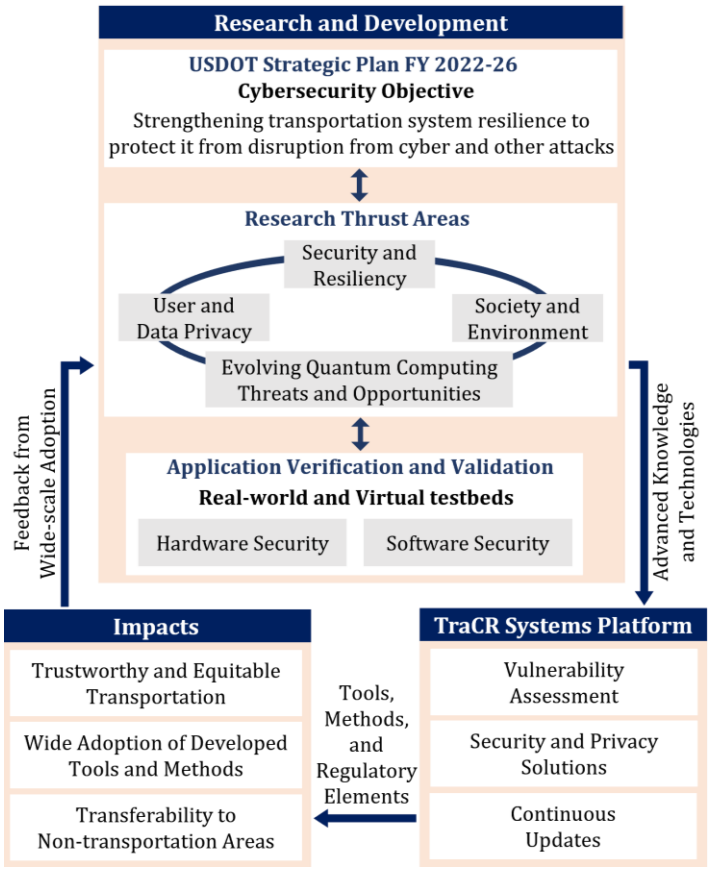

Figure 1. TraCR's Research Outlook and Impacts.

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.

TraCR's work will extend beyond hardware and software; we will also utilize the social sciences and other disciplines to address the policies, procedures, standards, social factors, legal aspects, and financing tools required to deploy cybersecurity tools in the public and private sectors. We will be just as committed to education, from elementary school through the doctoral level. In addition to offering courses, research opportunities, and mentoring programs at partner institutions, we will provide workforce training in other venues, such as two-year colleges. Utilizing the unique insights of our minority-serving institution partners (MSIs), we will reach out to those who might not otherwise participate in cybersecurity.

1.2. What was accomplished under these goals?

For this reporting period, the accomplishments are organized into three categories:
1) administrative accomplishments, 2) accomplishments related to the foundational project, and 3) accomplishments related to competitively selected research projects.

Administrative accomplishments

- We expanded our Advisory Board to include three additional members. Our board comprises industry and academic members from the transportation community. The TraCR advisory board members are listed below (new board members are highlighted in **bold**):

    - Dr. Kerry Buckley, MITRE Corp.
    - Cale Thorne, DMI Inc.
    - Dr. Richard S. Wilkins, Phoenix Technologies Inc.
    - Dr. Anuja Sonalker, STEER Tech.
    - Dr. Alireza Abbaspour, Qualcomm
    - **Fred Payne**, Carolinas Alliance 4 Innovation and Greenville County Council
    - **Gail Peay**, Director of Advocacy and Community Engagement, Habitat for Humanity
    - **Dr. Nadim Aziz**, Director SC EPSCoR State Program

- Jean Michel Tine was brought on board as the Minority Serving Institution (MSI) Coordinator starting January 2024. The role of the MSI coordinator will be to support and coordinate activities for TraCR faculty and students at our MSI partners, South Carolina State University (SCSU), Morgan State University (MSU), Benedict College (Benedict), and Florida International University (FIU) and in transportation-related disciplines and TraCR-related research.

- Development of TraCR's permanent office at the Clemson University International Center for Automotive Research (CU-ICAR) campus of Clemson University was completed, and our staff moved into the office in January 2024. The office is located at One Research Drive, Suite 414

A, Greenville, SC 29607.

Accomplishments related to 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. To this end, our foundational project team at Clemson decided to start with a transportation application-focused approach. The team has 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 SCSU, MSU, Benedict, FIU, the University of Alabama at Tuscaloosa (UA), the University of Texas at Dallas (UTD), Purdue University (Purdue), and the University of California, Santa Cruz (UCSC), as listed below. Each group's objective is to develop a platform that will help protect their respective transportation applications from cyber threats. The Clemson team is having recurring monthly meetings with all the groups to oversee the progress of the foundational project.
    - Autonomous vehicle safety systems – FIU and UA
    - Connected vehicle traffic signal system – FIU and UA
    - Dynamic transit operations – MSU and UTD
    - Electric charging stations management – Clemson, Benedict, and SCSU
    - Integrated multimodal electronic payment – Clemson, Benedict, and SCSU
    - V2V basic safety – Purdue and UCSC
    - Vulnerable road user safety – Purdue and UCSC
    - Transit security – MSU and UTD

- The CU team is working with Benedict and SCSU to develop 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). The team follows existing threat modeling strategies and tools to develop these platforms. The team is working to develop a seamless integration of network simulators and roadway traffic simulators to replicate real-world electric charging station management and integrated multimodal electronic payment applications. The team is closely investigating existing and evolving cyber threats and their mitigation strategies from renowned databases, such as MITRE ATT&CK, Common Vulnerabilities and Exposures (CVE), and Common Weakness Enumeration (CWE). These databases list known and emerging security flaws in software and hardware and their potential mitigations for any systems or applications. The team is working to develop strategies to map this knowledge base to transportation systems and infrastructure, starting with two transportation applications, as mentioned above.

- The UTD and the MSU teams have identified threats for Dynamic Transit Operations and Transit Security applications developed by the United States Department of Transportation under ARC-IT. The teams collected New York City Taxi data and assessed the performance of

the current state-of-the-art (SOTA) tabular data generation model. The experiments show that significant improvements need to be made to the model. The teams examined all the data/information flows and the service packages, and the details provided for the information flows and elaborated on the cyber security threats. The teams at UTD and MSU are utilizing MITRE's ATT&CK platform to identify all the threats. The teams are also examining the relevant NIST guidelines and frameworks to describe the threats.

Accomplishments related to competitively selected research projects

- TraCR Director Dr. Chowdhury (Clemson), and Associate Directors Drs. Comert (Benedict), Amini (FIU), Jeihani (MSU), Ukkusuri (Purdue), Mwakalonge (SCSU), Jones (UA), Cardenas (UCSC) and Thuraisingham (UTD) met virtually in November 2023 to evaluate research proposals submitted for competitive funding available during the 2023-2024 funding cycle.

- Fourteen research projects were selected for funding based on external reviews from the 15 submitted proposals to the Request for Proposals sent out in Fall 2023 for competitive funding available through TraCR. Clemson, Purdue and UA are leading three funded projects each, while FIU, MSU, SCSU, UCSC, and UTD each lead one project. Benedict is collaborating on seven of the selected projects. The Principal Investigators of the selected projects were notified in December 2023, and projects began on January 1st, 2024. Collaboration between consortium members was strongly encouraged; thus, each project includes at least one partner institution and the leading institution. The list of projects selected is provided below:

No.	Proposal Title	Principal Investigator	Co- PI's
1.	Intersectionality of Infrastructural Cybersecurity, Digital Equity and Social Agency	**Asha Layne,** Morgan State University	**Larry Liu,** Morgan State University; **Gurcan Comert**, Benedict College
2.	Cybersecurity Testbed for Connected and Autonomous Vehicles	**Satish Ukkusuri**, Purdue University	**Alvaro Cardenas, Daniel Fremont, Leilani Gilpin,** The University of California Santa Cruz; **Gurcan Comert**, Benedict College; **Mansoureh Jeihani,** Morgan State University; **Ronnie Chowdhury, M Sabbir Salek,** Clemson University
3.	Secure and Privacy-Preserving Federated Learning for Connected and Automated Vehicles	**Mohammadhadi Amini,** Florida International University	**Mansoureh Jeihani,** Morgan State University; **Farhad Shirani Chaharsooghi, Kemal Akkaya, Selcuk Uluagac,**

No.	Proposal Title	Principal Investigator	Co- PI's
			Florida International University
4.	A Multi-Resolution Simulation Platform for Transportation System Security Testing and Evaluation	**Yiheng Feng,** Purdue University	**Satish Ukkusuri,** Purdue University; **Mohammadhadi Amini,** **Kemal Akkaya,** Florida International University
5.	Finding Vulnerabilities of Autonomous Vehicle Stacks to Physical Adversaries	**Z. Berkay Celik,** Purdue University	**Alvaro Cardenas**, **Daniel Fremont,** The University of California Santa Cruz; **Satish Ukkusuri,** Purdue University
6.	Privacy-preserving Transportation Data Analytics Using Synthetic Data Generation	**Murat Kantarcioglu,** The University of Texas Dallas	**Alvaro Cardenas** , The University of California Santa Cruz; **Latifur Khan,** **Bhavani Thuraisingham,** The University of Texas Dallas; **Gurcan Comert,** Benedict College
7.	Adversarial Attacks against Camera-LiDAR Based Autonomous Driving Systems	**Cihang Xie,** The University of California Santa Cruz	**Alvaro Cardenas** , The University of California Santa Cruz; **Murat Kantarcioglu,** The University of Texas Dallas
8.	Policy Analysis and Guidance to Support Secure Transportation Cyber-Physical-Social Systems	**Steve Jones,** The University of Alabama Tuscaloosa	**Mizanur Rahman,** **Trayce Hockstad,** The University of Alabama; **Latifur Khan,** The University of Texas Dallas; **Ronnie Chowdhury,** **M Sabbir Salek,** Clemson University
9.	Building a Secure Electronic Control Unit Hardware Platform for Connected Vehicles	**Zhenkai Zhang,** Clemson University	**Gurcan Comert**, Benedict College; **Long Cheng,** Clemson University
10.	Multimodal In-Vehicle Sensor Fusion for Cyber-Secured Autonomous Navigation	**Mizanur Rahman,** The University of Alabama Tuscaloosa	**Ronnie Chowdhury,** **Long Cheng,** **M Sabbir Salek,** Clemson University
11.	A Zero Trust Architecture for Secure Connected and Autonomous Vehicles	**Long Cheng,** Clemson University	**Zhenkai Zhang,** Clemson University; **Gurcan Comert**, Benedict College
12.	Reinforcement Learning-Assisted Virtualized Security Framework for	**Jagruti Sahoo,** South Carolina State University	**Judith Mwakalonge,** **Nikunja Swain,** **Biswajit Biswal,**

No.	Proposal Title	Principal Investigator	Co- PI's
	CAVs		South Carolina State University; **Gurcan Comert**, Benedict College
13.	Secured Small-Key-Based Post Quantum Cryptographic Scheme for Blockchain-based VANET	**Mizanur Rahman,** The University of Alabama Tuscaloosa	**Ronnie Chowdhury,** **M Sabbir Salek,** **Yingjie Lao,** **Zhenkai Zhang,** **Shaozhi Li,** Clemson University
14.	Hybrid Classical-quantum AI Approach for Detecting Cyberattacks in Vehicles	**Shaozhi Li,** **Sumanta Tewari (Co-Lead),** Clemson University	**Ronnie Chowdhury,** **M Sabbir Salek,** Clemson University; **Vaneet Aggarwal,** **Satish Ukkusuri,** Purdue University; **Gurcan Comert**, Benedict College

The selected projects started on January 1st, 2024, and will be completed on December 31st, 2024. We are featuring here key progress from some of the above-selected projects. For each of the projects above, a quarterly progress report will be submitted to the TraCR administration by April 30th, 2024, which will be made available on the TraCR website. (https://www.clemson.edu/cecas/tracr/index.html).

- For project #3 listed above, the MSU team has devised an innovative hybrid privacy-preserving algorithm for countering adversarial attacks within Intelligent Transportation Systems (ITS), particularly focusing on object recognition. This algorithm represents a breakthrough, empowering all cyber-physical edge-client devices—such as autonomous vehicles (AVs)—and traffic control rooms to collectively refine their models while safeguarding the privacy of their individual datasets. Moreover, this hybrid algorithm can be used against data poisoning-based model replacement attacks and inference attacks throughout the training phase, ensuring robust security. Also, the FIU team has worked on the problem formulation of security and privacy challenges of federated learning algorithms for autonomous transportation systems. This problem formulation serves as a platform for the next steps, which include the development of solutions for these techniques.

- For project #6 listed above, the goal is to develop a synthetic data generation tool tailored for sharing privacy-preserving transportation data. The team has collected New York City (NYC) Taxi data as an initial mobility/transportation dataset. This dataset comprises records of taxi rides in NYC, capturing attributes such as pick-up and drop-off dates and times, locations, trip distances, itemized fares, rate types, payment methods, and passenger counts. The team assessed the performance of the current state-of-the-art (SOTA) tabular data generation model, CTGAN, using various metrics, including downstream tasks, Kolmogorov-

Smirnov statistics, Total Variation Distance, and Wasserstein distance between real and synthetic data. The team's experiments reveal a significant need for improvement in the current synthetic data generation models for accurately representing transportation data. The team utilized a SOTA tabular synthetic data generation to create synthetic taxi data, which was then used to train a machine learning model for predicting taxi ride fares. The results show a considerable disparity in predictive performance between models trained on real data versus those trained on synthetic data. This substantial performance gap, particularly evident in downstream tasks such as predicting itemized fares, underscores the inadequacy of the baseline SOTA synthetic data generation model for transportation data. As part of ongoing research, the team aims to develop a new synthetic mobility data generation tool specifically designed to accommodate the unique characteristics of transportation data. The team will model transportation routes as graphs and utilize specialized graph-generation tools to create synthetic mobility data. Additionally, the team will investigate whether existing attacks on synthetic data can be adapted for use with synthetic mobility and transportation data. To support this endeavor, the team has already completed an initial literature review on privacy attacks against synthetic data.

- For project #8 listed above, the goal is to identify the loopholes in Federal and State legislation to solve issues relating to data privacy and cybersecurity in the domain of autonomous vehicles, suggest additions or modifications to the existing set of legislation so that possible scenarios when they arise, can be taken care of. The team has curated state-level legislation resources and has summarized those resources using several large language models (LLMs), e.g., Gemini, ChatGPT, and Claude. All the recently enacted state-level legislations are collected from various online sources (e.g., The National Conference of State Legislatures or NCSL, and extensive databases like LexisNexis). For future usage, the team has also collected the proposed laws (but not necessarily enacted) for suggestive purposes (for example, if a law has been enacted, it could have been better to handle cybersecurity and data privacy cases in the domain of autonomous vehicles). The team has also collected federal legislation to analyze the coverage that the federal bills have regarding autonomous vehicles' cybersecurity and data privacy issues. The team has also curated a question dataset that is comprehensive in characteristics to pinpoint the loopholes in the existing legislation. Some of the sample questions are provided below:
    a. How do most states define critical infrastructure in the context of cybersecurity?
    b. Can you provide examples of penalties or fines imposed for non-compliance with cybersecurity requirements?
    c. How do states address data privacy concerns in the realm of cybersecurity?

  These questions are somewhat generic. The team is expanding this question set to pinpoint the inconsistencies in the legislation across states more concretely. The team has also developed a retrieval augmented generation (RAG) based pipeline to incorporate the most updated versions of legislation (e.g., recently enacted legislation) and to feed them to the LLMs for Question-Answering task(s). The team has validated the RAG pipeline preliminarily by adding additional relevant questions being asked to the LLMs to identify if relevant legislation is being retrieved as 'prompts' to our Q&A task. Some sample validation questions

are listed below:

a. What specific updates were made to the registration processes under Connecticut's Motor Vehicle Registration Act?
b. What is the purpose of establishing a joint legislative committee in Alabama to study self-driving vehicles?
c. What is the main objective of "The Road Repair and Accountability Act of 2017" in California?

These questions are curated specific to particular legislation and are used to crosscheck if the RAG model retrieves appropriate legislative summaries.

- For project #14, the Clemson team explored five shallow quantum circuits integrated within a convolutional neural network (CNN). Numeral training on the handwritten MNIST dataset reported superior classification performance of the hybrid quantum-classical CNN models. An in-depth analysis of the hybrid quantum-classical CNN models indicated the models' performance is attributable to their superior feature selection capabilities. The Clemson team then analytically developed a novel quantum activation function from the quantum circuit designs. This quantum activation function is able to harness quantum supremacy when incorporated within classical CNN models. These findings are being utilized by the team to develop a robust intrusion detection system for in-vehicle networks.

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

- As part of our workforce development/training activities, 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).

  - In October 2023, we hosted a seminar from Associate Director Dr. Gurcan Comert from Benedict College, who discussed **Simple Analytical Models for Estimating the Queue Lengths from Probe Vehicles at Traffic Signals II: A Combinatorial Approach for Nonparametric.**
  - Our December 2023 webinar featured Dr. Bhavani Thuraisingham from The University of Texas at Dallas, who talked about the work on **Integrating Cyber Security and Machine Learning for Applications in Transportation Systems**.
  - In January 2024, we featured Dr. Alvaro Cardenas from the University of California, Santa Cruz, in the webinar series. Dr. Alvaro's talk was **On Preventing, Detecting, and Responding to Attacks Against Autonomous Vehicles**.
  - In March 2024, Rachelle Beckner from Clemson University gave a talk on Mastering **Scientific Communication in the Digital Age: Strategies and Tools for Captivating Presentations and Articles in a TikTok-Dominated World.**
  - In April 2024, the webinar featured Dr. Paul Wang, a distinguished chair at Morgan State University, who discussed **Advances in Quantum Cryptography and Next Generation Quantum Internet.**

- Two new graduate students, Ms. Hannah Musau and Mr. Denis Ruganuza were brought on board at SCSU. The two students are collaborating with Benedict in research on security and resilience on both the foundational project and the competitively selected project, "*Reinforcement Learning-Assisted Virtualized Security Framework for CAVs*."

- Associate Director Dr. Hadi Amini from FIU participated in a two-day training program offered by STARTUP FIU for researchers interested in exploring future commercialization and technology transfer activities. Dr. Amini will use his training experience to specifically help with technology transfer from outcomes from research conducted through TraCR funds.

- The UTD team introduced a unit on Integrating AI and Cyber Security for Transportation Systems in a course on Data and Applications Security and Privacy offered during the spring 2024 semester at UTD.

- The UTD team has also introduced a new course in Generative AI and Large Language Models in which one unit focuses on security issues.

- Associate Director Dr. Bhavani Thuraisingham (UTD) delivered a featured address on Integrating Cyber Security and Artificial Intelligence for Transportation Systems at LLNL (Lawrence Livermore National Laboratory) for the Women in Data Science Conference in February 2024.

- Associate Director Dr. Bhavani Thuraisingham (UTD) delivered a featured address to the AI Student Society at UT Dallas (over 100 participants, including members from local companies) on Trustworthy AI and Applications to Transportation Systems in April 2024.

- Associate Director Dr. Bhavani Thuraisingham (UTD) delivered a featured address as part of the Grace Series Lecture Series on Trustworthy AI + Playing the Long Game for Career Success at UTD in April 2024.

- Luis Burbano, a Ph.D, student from UCSC, traveled to the Vehicle Security Conference (VehicleSec) 2024, in San Diego, CA.

- The MSU team collaborated with Dr. Paul Wang to coordinate a webinar on crypto algorithms and implementations and issues with existing encryption technologies in the quantum age, in addition to addressing quantum-safe security and privacy algorithms and the safe application of proposed algorithms in connected vehicles.

- The Clemson team has started working on developing e-learning modules on security engineering. These modules will be part of a stackable certification program and, once published, will be available to anyone around the world. The first e-learning module

comprises four lessons: i) Security Engineering, ii) Security Principles and Frameworks, iii) Cryptography, and iv) Threat Modeling.

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

- The center continues to maintain its website at https://www.clemson.edu/cecas/tracr/ to disseminate several outcomes.
  The website now includes a list and abstract of all competitively selected projects(available at: https://www.clemson.edu/cecas/tracr/research/projects.html) and information about our upcoming annual conference (see below). 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

- Associate Director Dr. Steven Jones (from UA) and Dr. Mizanur Rahman (co-PI at UA) and their research team attended the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., in January 2024 and presented five cybersecurity-related papers from research conducted through TraCR funds. Dr. Jones (from UA) and Dr. Salek (from Clemson) also presented an overview of TraCR to the TRB Joint Subcommittee on Cybersecurity.

- TraCR Director Dr. Ronnie Chowdhury, senior engineer Dr. M Sabbir Salek, MSI coordinator Jean Michel Tine, and two students supported by TraCR (from Clemson) attended the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., in January 2024. Dr. Salek presented a poster on a TraCR-supported project at the conference.

- TraCR Director Dr. Ronnie Chowdhury participated in the ARPA-I Listening Tour Workshop on February 9, 2024, in Atlanta, Georgia, hosted by Georgia Tech.

- Dr. Mizanur Rahman (co-PI at UA) and his research team conducted a live demonstration of cyber-resilient navigation technologies for autonomous vehicles that they developed through TraCR funds at the 2023 IEEE International Automated Vehicle Validation Conference, Austin, Texas, October 16-18, 2023. More information about the demonstration is available at: https://2023.iavvc.org/live-demonstrations.

- Associate Director Dr. Bhavani Thuraisingham (UTD) gave a seminar on TraCR-related research to UT Dallas AI Student Society titled Trustworthy AI for Transportation Systems.

- Dr. Berkay Celik (Purdue) was selected as the general chair of the Symposium on Vehicle Security and Privacy (VehicleSec 2024), co-located at the Network and Distributed System

Security (NDSS) Symposium, a top-tier security conference. More information can be found at https://www.ndss-symposium.org/ndss2024/co-located-events/vehiclesec/.

- TraCR hosted a technology demonstration for visitors from Habitat for Humanity and Goodwill on February 19th, 2024. Attendees were introduced to transportation cyber-physical-social systems (TCPSS) and self-driving cars by TraCR director, Dr. Ronnie Chowdhury and students. The attendees learned about: (1) hybrid classical-quantum deep learning models to detect adversarial attacks that affect the performance of the perception module of autonomous vehicles, (2) virtual traffic signal control with cloud-based quantum computers, and (3) distributed machine learning models or environmental emission detection with unmanned aerial vehicles.

- TraCR organized a hands-on workshop on quantum computing for undergraduate students at the Men of Color National Summit (2024). In addition, TraCR's Director, Dr. Ronnie Chowdhury, along with the Associate Directors, Dr. Judith Mwakalonge and Dr. Gurcan Comert, hosted a session on career and professional development titled "Opportunities for Careers and Capacity Building Resources in the Emerging Quantum Information Science" at the Men of Color National Summit (2024).

- TraCR Director Dr. Ronnie Chowdhury, senior engineer Dr. M Sabbir Salek, MSI coordinator Jean Michel Tine, and three students supported by TraCR (from Clemson) attended the 2024 SC EPSCoR conference and delivered two podium presentations and two posters.

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.

Plans for Training, Professional Development, and Outreach

- TraCR is hosting an Annual Conference scheduled for May 6-7. The conference will be held in Greenville, SC, at Clemson University's ICAR campus. The conference will include updates on research activities from the Associate Directors at our partner institutions. We also plan a student poster presentation session and a live demonstration session. In addition, the TraCR leadership will meet with the Advisory Board to discuss the center's progress and make strategic plans to widen the net of TraCR's impacts in the coming year. Details of the agenda and other logistics are available on the TraCR website: https://www.clemson.edu/cecas/tracr/news/conference.html.

- Dr. Ronnie Chowdhury (Center Director), Dr. Sabbir Salek (Senior Engineer/Tech Transfer Coordinator), and Ms. Megha Patel (Senior Program Manager) will attend the CUTC Summer

Meeting in South Padre Island, TX. (June 10th- 12th, 2024). TraCR faculties and students will attend and participate in the Future of Transportation Summit (FoT Summit 2024) to be held on August 13-15, 2024, in Washington DC, at the US DOT Headquarters.

- Luis Burbano, a Ph.D. student from UCSC, will give talks at Lund University and Chalmers University in Sweden about his work on TraCR.

- Associate Director Dr. Alvaro Cardenas (from UCSC) will give presentations at Queens University, Bristol University, and Cardiff University about his work on TraCR projects.

- Associate Director Dr. Bhavani Thuraisingham (from UTD) will give a keynote presentation at the ACM SACMAT Conference in May 2024 (a top-tier cyber security conference) on Trustworthy AI for Transportation Systems.

Plans for foundational project

- Since the mapping of possible attacks and their mitigation combined with NIST guidelines may present complicated many-to-many relationships, the UTD and MSU teams will work towards developing a Visualization Tool that will consolidate all the information about Transit Security, including the MITRE ATT&CK-related information and NIST guidelines as well as available tools. This tool will provide valuable assistance to those working in transportation systems (e.g., vehicle drivers) to realize underlying vulnerabilities of transit management systems and their potential mitigations. The UTD and MSU teams will simulate the subset of the threats and develop a demonstration system.

- The Clemson team will develop an in-the-loop simulation platform integrating a network simulator with a microscopic traffic simulator. This simulation platform will then be used to simulate two selected transportation applications, i.e., electric charging stations management and integrated multimodal electronic payment systems. A comprehensive threat modeling approach, following the existing databases for cyber vulnerabilities and cybersecurity framework, will be implemented to identify the threats related to software and hardware for the two selected applications.

Plans for competitively-selected projects

- Our team at SCSU is working on a comprehensive literature review of research on security and resilience through project #12 above, and the team is hoping to submit this literature review for publication soon.

- The FIU team has made progress on implementing the first version of privacy-preserving secure federated learning codes for the competitive project #3. The team is improving the code and planning to have the fully functioning code ready by the end of next quarter.

- For the competitive project #6, the UTD team will create a new graph-centric synthetic mobility data generation tool. The team will also assess the privacy safeguards of the newly developed tool by applying existing privacy attacks against synthetic datasets to the generated synthetic data. The team also plans to share our synthetic data generation code and the generated data online.

- For the competitive project #8, the UTD team will extract the answers/responses from different open-source LLMs and analyze the quality of the responses. The team will generate responses for a single question for all different states and the valid responses. Then, the team will cross-check the responses per state to indicate what legislation is missing on certain state levels. The team plans to validate the quality of our assessments by generating a factual database (e.g., a knowledge graph) built on factual textual information. Verification of the accuracy of the LLM-generated content will be done using structured knowledge of the legal domain (a specialized domain) (e.g., knowledge graphs). The team has also developed an RAG pipeline and plans to make it live/online (accessible via a website). The live website will be used to upload newer legislation, ask certain questions, and get responses using the entire pipeline.

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 at Santa Cruz (UCSC)
- The University of Texas at Dallas (UTD)

We have initiated the following collaborations during our first year:

Clemson is collaborating with the following entities:

- 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 the SUNTRAX Test Facility (https://suntraxfl.com).

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., who provided Spirent GSS9000, which is a hardware-in-the-loop Global Navigation Satellite Systems (GNSS) simulator package.

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

3. OUTPUTS:

3.1. Publications, conference papers, and presentations

Books, Book Chapters, and Journal Publications

1. Moore, E., Imteaj, A., Rezapour, S., and Hadi Amini, M., 2023. A Survey on Secure and Private Federated Learning Using Blockchain: Theory and Application in Resource-constrained Computing. IEEE Internet of Things Journal, 10, 21942-21958.
2. Chengula, T. J., Mwakalonge, J., Comert, G. and Siuhi, S., 2023. Improving road safety with ensemble learning: Detecting driver anomalies using vehicle inbuilt cameras. Machine Learning with Applications, 14, 100510.
3. Xie, S., Li, Z., Wang, Z. and Xie, C., 2023. On the Adversarial Robustness of Camera-based 3D Object Detection. Transactions on Machine Learning Research.
4. Indah, D. A., Mwakalonge, J., Comert, G. and Siuhi, S., 2024. Enhancing data efficiency for autonomous vehicles: Using data sketches for detecting driving anomalies. Machine Learning with Applications, 15, 100530.
5. Khan, S. M., Salek, M. S., Harris, V., Comert, G., Morris, E. A. and Chowdhury, M., 2024. Autonomous Vehicles for All? Journal on Autonomous Transportation Systems, 1, 1-8. (This work was partially supported by TraCR and C^2M^2)
6. Desai, H., and Kantarcioglu, M., 2024 Blockchains and Intelligent Transportation System Applications. In: Second Edition of Data Analytics for Intelligent Transportation Systems. Editors: Dey et al., Elsevier, **in press**.
7. 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**.
8. Comert, G., Amdeberhan, T., Begashaw, N., Medhin, N. and 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, **in press**.
9. Dasgupta, S., Irfan, M.S., Rahman, M. and Chowdhury, M., 2024. Modeling, detection and mitigation of GNSS spoofing attack in ground transportation systems. In: Data Analytics for Intelligent Transportation Systems, 2nd Edition, Elsevier, **in press**.

10. 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, Special Issue on Cybersecurity and Resiliency for Transportation Cyber-Physical System. ACM Journal on Autonomous Transportation Systems (JATS), **under review**.
11. Hockstad, T., Rahman, M., Jones, S., and Chowdhury, M. 2024. A Regulatory Gap Analysis in Transportation Cybersecurity and Data Privacy. Transport Policy Journal, **under review**.
12. 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 review**.
13. Mia, M. J., Amini, M. H., 2024. A Secure Object Detection Technique for Intelligent Transportation System. IEEE Open Journal of Intelligent Transportation Systems, **under review**.
14. Li, S., Salek, M. S., Wang, Y., Chowdhury, M., 2024. Quantum-inspired Activation Functions in the Convolutional Neural Network. Nature Computational Science, **under review**.

Conference Papers/Presentations

1. Salek, M. S., Chowdhury, M. Cybersecurity of Transportation Systems. Presented at the Appalachian Leadership Institute Panel, Spartanburg, SC, December 2023.
2. Aldeen, M., MohajerAnsari, P., Ma, J., Chowdhury, M., Cheng, L., Pese, M.D. WIP: A First Look at Employing Large Multimodal Models Against Autonomous Vehicle Attacks. Symposium on Vehicles Security and Privacy (VehicleSec) 2024. San Diego, CA, February 2024. https://dx.doi.org/10.14722/vehiclesec.2024.23044
3. Tine, J. M., Puspa, S. N., Majumdar, R., Comert, G., Chowdhury, M. and Lao, Y. Threats of Trojan Incursion in Transportation Hardware. Presented at the 2023 IEEE International Automated Vehicle Validation Conference (IAVVC), Austin, TX, October 2023.
4. Halim, S., Hossain, D., Khan, L., Singhal, A., Ochiai, H., Hamlen, K., Kadobayashi, Y. Securing Smart Vehicles through Federated Learning. Presented at the 16th International Symposium on Foundations & Practice of Security (FPS – 2023), France, December 2023.
5. Hossain, M. Z., Imteaj, A., Zaman, S., Shahid, A. R., Talukder, S., and Amini, M. H. FLID: Intrusion Attack and Defense Mechanism for Federated Learning Empowered Connected Autonomous Vehicles (CAVs) Application. Presented at the 2023 IEEE Conference on Dependable and Secure Computing (DSC), Tampa, FL, November 2023.
6. Hockstad, T., Rahman, M., Jones, S., Chowdhury, M. A Regulatory Gap Analysis in Transportation Cybersecurity and Data Privacy. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
7. Dasgupta, S., Hassan Shakib, K., Rahman, M. Experimental Validation of Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
8. Hassan Shakib, K., Kiesewetter, L., Rahman, M., Shah, K. Examining Safety and Cybersecurity for Urban Air Mobility Operations. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.

9. Dasgupta, S., Ahmed, A., Rahman, M. Unveiling the Stealthy Threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling the Resilience. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
10. Noman, S., A., Atkison, T., Sami Irfan, M., Rahman, M. A Predictive Approach for Sybil attack Detection for a Waiting Time-Based Adaptive Traffic Signal Controller. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
11. Xue, J., Ukkusuri, S. Generating Network-Level Dynamic Traffic Equations Using Symbolic Regression. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
12. 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. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
13. Chen, H., Chen, S., Li, W., Yang, W., and Feng, Y. Impact Analysis of Inference Time Attack Of Perception Sensors on Autonomous Vehicles. Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
14. Ying, J., Feng, Y., Algred, Q., Chen, Z. and Mao, M. Modeling and Detecting Falsified Vehicle Trajectories Under Data Spoofing Attacks Presented at the 103rd Annual Meeting of the Transportation Research Board, Washington, D.C., January 2024.
15. Musau, H. M., Mwakalonge, J., Comert, G., & Siuhi, S. Analyzing The Impact of COVID-19 Pandemic on Factors Affecting School Travel Mode Choice in the United States. Presented at the 4th IEEE Forum for Innovative Sustainable Transportation Systems, Riverside, CA, February 2024. (Partially supported by TraCR)
16. Osei, E., Mwakalonge, J., Comert, G., & Siuhi, S. Human and Animal Detection in Electric and Autonomous Vehicles Using Quantum Computing and Advanced Machine Learning Techniques. Presented at the 4th IEEE Forum for Innovative Sustainable Transportation Systems, Riverside, CA, February 2024. (Partially supported by TraCR)
17. Omulokoli, P. O., Mwakalonge, J. L., Comert, G., Siuhi, S. Optimal location selection for electric vehicle infrastructure using location-allocation models with socio-economic considerations. Presented at the 4th IEEE Forum for Innovative Sustainable Transportation Systems, Riverside, CA, February 2024. (Partially supported by TraCR)
18. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. Sustainable Freight Through Topological Data Analysis: Optimizing Freight Routes for Environmental Impact. Presented at the 4th IEEE Forum for Innovative Sustainable Transportation Systems, Riverside, CA, February 2024. (Partially supported by TraCR)
19. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. An Investigation of Location-based Factors Influencing Electric Vehicles Charging Behavior. Presented at the 4th IEEE Forum for Innovative Sustainable Transportation Systems, Riverside, CA, February 2024. (Partially supported by TraCR)
20. Chengula, T. J., Mwakalonge, J., Comert, G., & Siuhi, S. Examination of Urban Micromobility Dynamics: A Geospatial Analysis of Scooter Crash Hotspots and Temporal Patterns.

Presented at the 4th IEEE Forum for Innovative Sustainable Transportation Systems, Riverside, CA, February 2024. (Partially supported by TraCR)

21. Musau, H. M., Mwakalonge, J., Comert, G., & Siuhi, S. Analysis of Twitter Data on COVID-19 and School Transportation: A Topic Modeling Approach. Presented at the 53rd Annual Meeting of Southeast Decision Sciences Institute (SEDSI), Charleston, SC, February 2024. (Partially supported by TraCR)
22. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. Leveraging Quantile Sketches for Efficient Management of Transportation Big Data: An Experimental Approach. Presented at the 53rd Annual Meeting of Southeast Decision Sciences Institute (SEDSI), Charleston, SC, February 2024. (Partially supported by TraCR)
23. Omulokoli, P. O., Mwakalonge, J. L., Comert, G., Siuhi, S. A causal inference study of crashes at Highway-Rail Grade crossings. Presented at the 53rd Annual Meeting of Southeast Decision Sciences Institute (SEDSI), Charleston, SC, February 2024. (Partially supported by TraCR)
24. Sulle, M., Mwakalonge, J.L., Comert, G., Siuhi, S., Roberts, J. Analysis of Distracted Pedestrians Crossing Behavior: An Immersive Virtual Reality Application. Presented at the 53rd Annual Meeting of Southeast Decision Sciences Institute (SEDSI), Charleston, SC, February 2024. (Partially supported by TraCR)
25. Chengula, T. J., Mwakalonge, J., Comert, G., & Siuhi, S. Exploring Autonomous Vehicle Disengagements Via Latent Dirichlet Allocation Analysis: A Natural Language Processing Approach. Presented at the 53rd Annual Meeting of Southeast Decision Sciences Institute (SEDSI), Charleston, SC, February 2024. (Partially supported by TraCR)
26. Chengula, T. J., Mwakalonge, J., Comert, G., Sulle, M., & Siuhi, S. Enhancing Advanced Driver Assistance Systems Through Explainable Artificial Intelligence for Driver Anomaly Detection Presented at the 50th Annual Convention, National Society of Black Engineers, Atlanta, GA, March 2024. (Partially supported by TraCR)
27. Musau, H. M., Mwakalonge, J., Comert, G., Sulle, M., & Siuhi, S. Evaluating Factors Influencing School Travel Mode Choice in the United States Using Explainable Artificial Intelligence. Presented at the 50th Annual Convention, National Society of Black Engineers, Atlanta, GA, March 2024. (Partially supported by TraCR)
28. Sulle, M., Mwakalonge, J. L., Comert, G., Siuhi, S., Roberts, J. Analysis of Distracted Pedestrians Crossing Behavior: An Immersive Virtual Reality Application. Presented at the 50th Annual Convention, National Society of Black Engineers, Atlanta, GA, March 2024. (Partially supported by TraCR)
29. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. Sustainable Freight Through Topological Data Analysis: Optimizing Freight Routes for Environmental Impact. Presented at the 50th Annual Convention, National Society of Black Engineers, Atlanta, GA, March 2024. (Partially supported by TraCR)
30. Ruganuza, D., Omulokoli, P. O., Mwakalonge, J. L., Comert, G., Siuhi, S. Enhancing Road Safety: Investigating Animal-Autonomous Vehicle Collision Avoidance Using F1/10 Vehicles to Warn Human Drivers and Nearby Traffic. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
31. Omulokoli, P. O., Mwakalonge, J. L., Comert, G., Siuhi, S. Explanatory analysis of

spatiotemporal distribution trends of electric vehicle charging stations in two cities in South Carolina. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)

32. Omulokoli, P. O., Mwakalonge, J. L., Comert, G., Siuhi, S. A causal inference study of crashes at Highway-Rail Grade crossings. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
33. Musau, H. M., Mwakalonge, J., Comert, G., Sulle, M., & Siuhi, S. Analysis of Twitter Data on COVID-19 and School Transportation: A Topic Modeling Approach. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
34. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. Sustainable Freight Through Topological Data Analysis: Optimizing Freight Routes for Environmental Impact. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
35. Osei, E., Mwakalonge, J., Comert, G., Siuhi, S. Developing computer vision and sensor models for Parking facilities using Machine Learning techniques: Optimizing Parking Space Allocation. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
36. Chengula, T. J., Mwakalonge, J., Comert, G., Sulle, M., & Siuhi, S. Enhancing Advanced Driver Assistance Systems Through Explainable Artificial Intelligence for Driver Anomaly Detection. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
37. Sulle, M., Mwakalonge, J., Comert, G., Siuhi, S., Roberts, J. Cybersecurity Threats in Autonomous Vehicle Technologies: Perceptions and Preparedness, A Case Study. Presented at 2024 STEM Showcase, South Carolina State University, Orangeburg, SC, March 2024. (Partially supported by TraCR)
38. Musau, H. M., Mwakalonge, J., Comert, G., & Siuhi, S. A national survey on the effect of the COVID-19 pandemic on school travel in the US: Parents perspective. Presented at the Safe Mobility Conference, Chapel Hill, NC, March 2024. (Partially supported by TraCR)
39. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. Conditional Density Estimation for CMV Crash Severity Analysis and uncertainty Quantification in Work Zones. Presented at the Safe Mobility Conference, Chapel Hill, NC, March 2024. (Partially supported by TraCR)
40. Chengula, T. J., Mwakalonge, J., Comert, G., & Siuhi, S. Spatial Instability of Crash Prediction Models: A Case of Scooter Crashes. Presented at the Safe Mobility Conference, Chapel Hill, NC, March 2024. (Partially supported by TraCR)
41. Tine, J.-M. The Ethical Integration of Artificial Intelligence in Civil Engineering. Presented at the 2024 ASCE Symposium, Charlotte, NC, April 2024.
42. 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.
43. 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.

44. Puspa, S. N., Chowdhury, M. Hardware Trojan in Transportation. Presented at the 2024 SC EPSCoR Conference, Columbia, SC, April 2024.
45. Omulokoli, P. O., Mwakalonge, J.L, Comert, G., Siuhi, S. Spatiotemporal Modeling for Enhanced Road Safety: Bayesian Hierarchical Approach with INLA-SPDE in Analyzing Large Truck Crashes, Texas (2016-2021). Presented at the 65th International Meeting of the Transportation Research Forum, Arlington, VA, April 2024.
46. Ruganuza, D., Omulokoli, P. O., Mwakalonge, J. L., Comert, G., Siuhi, S. Enhancing Road Safety: Investigating Animal-Autonomous Vehicle Collision Avoidance Using F1/10 Vehicles to Warn Human Drivers and Nearby Traffic. Presented at the 65th International Meeting of the Transportation Research Forum, Arlington, VA, April 2024.
47. Sulle, M., Mwakalonge, J. L., Comert, G., Siuhi, S., Roberts, J. Analysis of Distracted Pedestrians Crossing Behavior: An Immersive Virtual Reality Application. Presented at the 65th International Meeting of the Transportation Research Forum, Arlington, VA, April 2024.
48. Osei, E., Mwakalonge, J. L., Comert, G., Siuhi, S. Developing Computer Vision and Sensor Models for Parking Facilities Using Machine Learning Techniques: Optimizing Parking Space Allocation. Presented at the 65th International Meeting of the Transportation Research Forum, Arlington, VA, April 2024.
49. Sulle, M., Mwakalonge, J. L., Comert, G., Siuhi, S., Roberts, J. Evaluating the Environmental Impact of Connected Autonomous Vehicles: Combustion Engine vs Electric Vehicles. Presented at the 2024 Southern District of ITE Annual Meeting, Wilmington, NC, April 2024.
50. Omulokoli, P. O., Mwakalonge, J. L, Comert, G., Siuhi, S. Spatiotemporal Modeling for Enhanced Road Safety: Explanatory analysis of spatiotemporal distribution trends of electric vehicle charging stations in two cities in South Carolina. Presented at the 2024 Southern District of ITE Annual Meeting, Wilmington, NC, April 2024.
51. Sulle, M., Mwakalonge, J.L., Comert, G., Siuhi, S., Roberts, J. Cybersecurity Threats in Autonomous Vehicle Technologies: Perceptions and Preparedness, A Case Study. Presented at the SC EPSCoR State Conference, Columbia SC, April 2024.
52. Musau, H. M., Mwakalonge, J., Comert, G., Sulle, M., & Siuhi, S. Evaluating Factors Influencing School Travel Mode Choice in the United States Using Explainable Artificial Intelligence. Presented at the SC EPSCoR State Conference, Columbia SC, April 2024.
53. Ruganuza, D., Omulokoli, P. O., Sulle, M, Mwakalonge, J. L., Comert, G., Siuhi, S. Creating a Comprehensive Dataset to Explore Retroreflectivity Degradation in Traffic Signs: Incorporating Environmental Factors. Presented at the 2024 SC EPSCoR State Conference, Columbia, SC, April 2024.
54. Indah, D. A., Mwakalonge, J. L., Comert, G., Siuhi, S. Conditional Density Estimation for CMV Crash Severity Analysis and uncertainty Quantification in Work Zones. Presented at the 2024 SC EPSCoR State Conference, Columbia, SC, April 2024.
55. Zhang, L., Burbano, L., Chen, X., Cardenas, A. A., Drager, S., Adderson, M., and Kong, F. Fast Attack Recovery for Stochastic Cyber-Physical Systems. To be presented at the IEEE Real-Time and Embedded Technology and Applications Symposium, Hong Kong, China, May 2024.

3.2. 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.

3.3. Technologies or techniques

Dr. Mizanur Rahman and his research team from the University of Alabama, Tuscaloosa, AL, conducted a live demonstration of cyber-resilient navigation technologies for autonomous vehicles at the 2023 IEEE International Automated Vehicle Validation Conference, Austin, TX, October 2023 (more information is available at: https://2023.iavvc.org/live-demonstrations).

3.4. Inventions, patent applications, and/or licenses

Nothing to report yet.

4. OUTCOMES:

- During this reporting period, the FIU team progressed toward modeling the privacy-preserving and secure federated learning algorithms for intelligent transportation systems. Specifically, the team leveraged two solutions to address privacy and security challenges. The team's hybrid solution integrates two state-of-the-art models to protect the privacy of the global machine learning models. Also, it isolates the potential adversarial clients (autonomous vehicles) in a distributed setting. The FIU team is also collaborating with other institutions within TraCR. The FIU team is also collaborating with the MSU team to share knowledge on cybersecurity and transportation engineering aspects of the team's project. Their input has been essential to ensure the developed algorithms are tailored to transportation systems.

- The Benedict team is setting up CUBEs at the Benedict campus for data generation (testbed) for communication signal attenuation due to cyber-attacks. During this setup, the team collaborated with Microtik company. These products help to understand and be aware of transportation issues and technology development and to use such for more efficient transportation systems. They not only increase the body of knowledge but may also improve processes for safety and energy use as well as equity.

- Dr. Mizanur Rahman (co-PI at UA) received the prestigious Faculty Early Career Development (CAREER) Award from the National Science Foundation (NSF)'s Secure & Trustworthy Cyberspace (SaTC) program of the Division of Computer and Network Systems, titled "CAREER: Cyber Resilient Navigation for Autonomous Systems under Threat Uncertainties and Contested Environments." Dr. Rahman aims to advance the scientific discovery of fundamental dynamics in cyber threat uncertainties for autonomous navigation under evolving attack surfaces in formulating a robust, efficient, flexible, and reliable positioning and navigation system.

- In collaboration with other partners, the MSU team developed threat models based on industry standards such as MITRE and NIST to enhance the understanding of potential cyber threats in transit operations. This knowledge aids in creating robust security measures to safeguard transit systems against cyber-attacks.

- For one of the competitively selected projects, the MSU team finalized the framework for the Cyber Security Testbed, incorporating components like METS-R SIM and CARLA, providing a comprehensive platform for testing, and validating cyber security measures for CAVs. This facilitates identifying and mitigating vulnerabilities, ultimately improving the resilience of CAV systems against cyber threats.

- For another competitively selected project, the novel hybrid privacy-preserving algorithm developed by MSU, and partners enables collaborative model training while maintaining data privacy in ITS. By defending against adversarial attacks and ensuring security against data poisoning and inference attacks, this algorithm promotes the adoption of federated

learning in real-world transportation scenarios, fostering trust and collaboration among stakeholders.

5. IMPACTS:

TraCR was established last year, and this is our second reporting period for the semi-annual progress report. Our activities have had several impacts already, highlighted below, and we expect to see a significant impact soon with the initiation of several TraCR-supported competitively selected research projects.

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

- The FIU team has developed a novel hybrid privacy-preserving algorithm to safeguard against malicious attacks in Intelligent Transportation Systems, considering object recognition as a downstream machine-learning task. The impact of this project is to enhance transportation safety. By developing robust threat models and frameworks for cyber security testing, the program will improve the safety and reliability of transportation systems. This includes transit operations, connected and automated vehicles (CAVs), and intelligent transportation systems (ITS), where vulnerabilities to cyber-attacks pose significant risks. Implementing these measures enhances the resilience of transportation systems, minimizing disruptions and ensuring passenger safety. Through the implementation of advanced cyber security measures and privacy-preserving federated learning algorithms, the program has bolstered the durability and resilience of transportation infrastructure. By identifying and mitigating potential cyber threats and adversarial attacks, the program helps fortify the integrity and longevity of transportation systems, reducing the likelihood of system failures and enhancing overall durability. The program's research outputs serve as valuable educational resources, contributing to the advancement of transportation education. By disseminating knowledge about cyber security challenges in transit operations, CAVs, and ITS, the program enhances the understanding of emerging threats among transportation professionals, researchers, and students. This fosters a more informed and proactive approach to addressing security issues in transportation.

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

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

During the reporting period, due to the time needed to process and set up the sub-award at FIU, the FIU team could not process student contracts in time and thus was slightly behind on spending. The team will use the excess funds to support students during the upcoming reporting period.

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.