Citation Evidence Report

EB-1B Petition — Outstanding Professor or Researcher

8 CFR § 204.5(i)(3) · Authorship + Original Contributions

Srivalli Boddupalli

Lucid Motors, University of Florida

Google Scholar profile

Generated 2026-05-21 by CiteMap. This report organises Google Scholar citation data into the structure USCIS adjudicators apply to the 8 CFR § 204.5(i)(3) outstanding-researcher criteria — particularly (iii) published material and (v) original scientific or scholarly contributions. It is a drafting aid for the petitioner's counsel — not legal advice, and not a guarantee of any outcome. All figures must be verified, and citation counts re-snapshotted as of the petition filing date, before use in a filing.

A. Overview & Filtering Statement

199	231	17	7
Citing papers mapped	Citation edges	Home papers mapped	h-index (GS)

Filtering statement — methodology & limits

Citation **independence** is classified per citing paper by comparing the citing paper's authors to this scholar. *Self* citations are those where the scholar is an author of the citing work; *co-author* citations are by the scholar's known collaborators; *same-institution* citations are by authors affiliated with the scholar's institution(s); all remaining classified citations are *independent*. Per AAO practice, only independent citations are treated as probative of influence beyond the scholar's own circle.

Known limitations — counsel must verify. (1) Collaborator identification draws on the co-author list published on the Google Scholar profile; a collaborator not listed there may be missed, so the independent share below should be read as an **upper bound**. (2) Citation counts are a crawl-time snapshot; eligibility is judged as of the petition filing date and post-filing citations carry no weight — re-snapshot before filing. (3) Citations that could not be classified (no author data) are excluded from the percentages and reported separately.

B. Citation Independence

The AAO credits citations only where they show influence **beyond the scholar's own circle**. Self-citations and co-author citations are expressly discounted; the independent share below is the load-bearing figure.

84.3% independent of 51 classified citing papers

Citation type	Count
Independent	43
Self-citation	3
Co-author	5
Same-institution	0

148 citing papers could not be classified (no author data) and are excluded from the percentages above.

C. Significant Contributions & Their Citation Evidence

Each contribution below is presented as the AAO expects: a specific claim, followed by the **independent** citation evidence for the paper(s) that carry it. Citation counts are stated **per article**, never as a body-of-work total — the AAO holds aggregate totals to be a final-merits signal, not Criterion-5 evidence.

Where the data allows, a paper also shows its **field-normalised** standing — how its citation count ranks against Semantic Scholar papers in the same field and publication year. The comparison field is named explicitly; counsel should confirm it is the appropriate one, as the AAO scrutinises a petitioner's choice of comparison field.

Contribution 1

Claim — Contribution 1

The researcher established a foundational framework for automotive system security, subsequently advancing resilient control mechanisms for autonomous vehicles against adversarial threats.

CLAIM: The researcher's contribution centers on securing emergent automotive systems, anchored by a 2019 tutorial paper that outlines practice perspectives and has garnered 33 citations. This core work serves as the basis for subsequent research into resilient autonomous vehicle technologies.

ORIGINALITY: The titles indicate a progression from general security perspectives to specific technical solutions. The researcher appears to have addressed the gap between theoretical security frameworks and practical resilience in cooperative adaptive cruise control and perception systems, applying machine learning to mitigate adversarial risks in connected autonomous vehicles.

SIGNIFICANCE: The line of work demonstrates substantial impact, with the 2022 follow-up on resilient control receiving 90 citations. Furthermore, analysis of 51 citing papers reveals that 84.3% originate from independent researchers, suggesting broad adoption and recognition of these security frameworks beyond the researcher's immediate circle.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 27 · **1 flagged influential by Semantic Scholar**

CORE PAPER

Security of emergent automotive systems: A tutorial introduction and perspectives on practice

2019 · IEEE Design & Test 36 (6), 10-38, 2019 · 33 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	ATHENA: An In-vehicle CAN Intrusion Detection Framework Based on Physical Characteristics of Vehicle Systems	Beijing Jiaotong University, Chongqing University, Harbin Institute of Technology	China	**Influential**
2	DriveGuard: Robustification of automated driving systems with deep spatio-temporal convolutional autoencoder	University of Cyprus	Cyprus	Background

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

Resilient cooperative adaptive cruise control for autonomous vehicles using machine learning

2022 · IEEE Transactions on Intelligent Transportation Systems 23 (9), 15655-15672, 2022 · 90 citations (GS)

Field-normalised: 53 Semantic Scholar citations place it in the top 10% of Computer Science papers from 2022 indexed by Semantic Scholar, by citation count.

No.	Citing paper	Citing institution(s)	Country	S2
1	A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks	University of Luxembourg	Luxembourg	Background
2	Roadmap for cybersecurity in autonomous vehicles	Colorado State University	United States	—

No.	Citing paper	Citing institution(s)	Country	S2
3	Communication-efficient MARL for platoon stability and energy-efficiency co-optimization in cooperative adaptive cruise control of CAVs	BYD Auto, Southeast University, Tongji University	China, United Kingdom, United States	—
4	A cyberattack detection-isolation algorithm for CAV under changing driving environment	Texas Tech University, Veer Surendra Sai University of Technology	India, United States	—
5	Safe and Secure Control of Connected and Automated Vehicles: An Event-Triggered Control Approach using Trust-Aware Robust Control Barrier Functions	Boston University, Massachusetts Institute of Technology	United States	—
6	Anomaly detection framework for securing next generation networks of platoons of autonomous vehicles in a vehicle-to-everything system	Indiana University-Purdue University Indianapolis	United States	Background
7	Perspective: A Novel Resilient Cybersecurity Management System for Connected and Automated Vehicles	Beihang University	China	—
8	To act or not to act: An adversarial game for securing vehicle platoons	CSIRO Data61, University of Melbourne	Australia	**Methodology**
9	Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles	Tongji University	China	**Methodology**
10	Secure control of connected and automated vehicles using trust-aware robust event-triggered control barrier functions	Boston University, Massachusetts Institute of Technology	United States	—
11	Machine learning-based detection and mitigation of cyberattacks in adaptive cruise control systems	School of Traffic and Transportation, Shijiazhuang Tiedao University, Wannan Medical College	China	—
12	Balancing safety and security in autonomous driving systems: A machine learning approach with safety-first prioritization	University of Guilan, University of Tehran	Iran	—
13	A proposed reinforcement learning approach via discrete control reformulation and multi-step double DQN for adaptive cruise control in electric vehicles	Arab Academy for Science and Technology and Maritime Transport	Egypt	—
14	Adaptive radial basis function sliding mode control for platoons under DoS attacks	The University of Wollongong, Zhengzhou Normal University	Australia, China	—
15	Trust-aware resilient control and coordination of connected and automated vehicles	Boston University, Massachusetts Institute of Technology	United States	Background
16	Hybrid cyber-resilient control for networked autonomous vehicles	Sivas University of Science and Technology	Turkey	—
17	Big Data and Machine Learning in Autonomous Vehicle Navigation: Challenges and Opportunities	Universiti Teknologi MARA	Malaysia	—

No.	Citing paper	Citing institution(s)	Country	S2
18	Adaptive Cruise Control in Autonomous Vehicles: Challenges, Gaps, Comprehensive Review, and, Future Directions	KLE Technological University	India	—
19	Resilient Interval Observer-Based Control for Cooperative Adaptive Cruise Control under FDI Attack	University of Tulsa	United States	—
20	Securing cyber-physical systems: Physics-enhanced adversarial learning for autonomous platoons	CSIRO Data61, University of Melbourne	Australia	**Methodology**
21	Advanced IoT-based Algorithms for Improved Object Detection and Navigation in Autonomous Vehicles	Saveetha School of Engineering, SRM Valliammai Engineering College	India	—
22	Exploring Attack Resilience in Distributed Platoon Controllers with Model Predictive Control	University of Florida	United States	—
23	Machine Learning Applications in V2X Networks: a systematic review	Instituto Federal de Educação, Ciência e Tecnologia da Bahia, Universidade Federal da Bahia, Universidade Federal do Recôncavo da Bahia	Brazil	—
24	Adaptive Learning Paths: Implementing Machine Learning to Personalize Curriculum Development in Multicultural Classrooms	Politeknik LP3I Makassar, Universitas Almarisah Madani	Indonesia	—
25	A New Adaptive Cruise Control Strategy Considering Road Conditions	Shiraz University	Iran	—

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Citing-text excerpts — how the field used this work

METHODOLOGY To act or not to act: An adversarial game for securing vehicle platoons

"The assumption that sensory inputs are trustworthy in the context of detecting communication-based attacks is prevalent in the literature [16], [17]."

METHODOLOGY Systematic assessment of cyber-physical security of lane keeping control system for autonomous vehicles

"Resilient Control [28] 2021 Adaptive resilient event-triggered control against DoS attacks [29] 2021 Nonlinear resilient path following control against DoS attacks [30] 2022 Resilient CACC for autonomous vehicles [19] 2022 Attack-resilient lateral stability control for electric vehicles"

METHODOLOGY Securing cyber-physical systems: Physics-enhanced adversarial learning for autonomous platoons

"We extend the message falsification attacks [2,19] from only affecting communication messages to attacking both communication and sensor observations [4] in a subtle way and name it vanilla false data injection (v-FDI)."

FOLLOW-UP WORK

Resiliency of Connected Autonomous Vehicle Applications Against Perception Security Adversaries

2022 · University of Florida, 2022 · 0 citations (GS)

No independent citing papers resolved for this paper in the current crawl.

Contribution 2

Claim — Contribution 2

The researcher developed a framework for real-time detection and mitigation of communication attacks in connected autonomous vehicles, extending this work to address security resiliency and validation challenges.

The researcher's contribution centers on enhancing the security of connected autonomous vehicle applications, anchored by the 2019 paper 'Redem: Real-time detection and mitigation of communication attacks in connected autonomous vehicle applications.' This core work established a foundation for identifying and neutralizing threats in real-time vehicular communications.

This line of work appears to address the critical gap in securing dynamic vehicular networks against evolving cyber threats. The titles suggest a progression from immediate attack mitigation to broader strategic concerns, as evidenced by follow-up papers in 2022 and 2023 that explore machine learning for security resiliency and approaches for security validation. This indicates a comprehensive approach to both reactive defense and proactive system hardening.

The significance of this research is reflected in its uptake by the academic community. The core paper has garnered 18 citations, while the follow-up works have received additional citations. Notably, 84.3% of the citing papers originate from independent researchers, suggesting that this work has influenced scholars outside the researcher's immediate circle and contributed meaningfully to the field of vehicular cybersecurity.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 6

CORE PAPER

Redem: Real-time detection and mitigation of communication attacks in connected autonomous vehicle applications

2019 · IFIP international Internet of Things conference, 105-122, 2019 · 18 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	A survey on machine learning-based misbehavior detection systems for 5g and beyond vehicular networks	University of Luxembourg	Luxembourg	Background
2	On data fabrication in collaborative vehicular perception: Attacks and countermeasures	University of California, Irvine, University of Michigan	United States	—
3	Attention in Motion: Secure Platooning via Transformer-based Misbehavior Detection	KTH Royal Institute of Technology, Lenovo	China, Sweden	—
4	Stealthy Data Fabrication in Collaborative Vehicular Perception	University of Michigan	United States	—
5	Evaluation of the architecture alternatives for real-time intrusion detection systems for connected vehicles	Iowa State University	United States	—

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

FOLLOW-UP WORK

Machine Learning for Security Resiliency in Connected Vehicle Applications

2023 · Machine Learning and Optimization Techniques for Automotive Cyber-Physical ..., 2023 · 1 citations (GS)

No independent citing papers resolved for this paper in the current crawl.

FOLLOW-UP WORK

Resiliency in connected vehicle applications: challenges and approaches for security validation

2022 · Proceedings of the Great Lakes Symposium on VLSI 2022, 475-480, 2022 · 3 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Exploring Attack Resilience in Distributed Platoon Controllers with Model Predictive Control	University of Florida	United States	—

Independent citing papers only; self- and co-author citations excluded. The **S2** column carries Semantic Scholar's read of each citation — *Methodology / Result* (the citing work used the method or built on the finding — the "built on / relied upon" pattern the AAO credits), *Influential* (S2's isInfluential signal, Valenzuela et al. 2015), or *Background* (a passing mention).

Contribution 3

Claim — Contribution 3

The researcher developed Autohal, a pioneering exploration platform for ranging sensor attacks on automotive systems, establishing a foundational framework for vehicular security research.

The researcher's core contribution centers on the development of Autohal, an exploration platform for ranging sensor attacks on automotive systems published in 2022. This work serves as the foundation for a broader line of inquiry into vehicular security, as evidenced by subsequent publications that expand upon these initial findings.

This line of work appears to address the need for practical, hands-on tools to understand and mitigate physical-layer vulnerabilities in modern vehicles. The progression from the core Autohal platform to follow-up studies on functional safety standards and vehicular communication attacks suggests a comprehensive approach to identifying and analyzing security gaps across different automotive subsystems.

The significance of this contribution is reflected in its adoption by the broader academic community. With 14 citations for the core paper and additional citations for related works, the research has garnered attention from independent scholars. Notably, 84.3% of the citing papers originate from independent researchers, indicating that the work has influenced peers outside the researcher's immediate institution and collaboration network.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 0

CORE PAPER

Autohal: An exploration platform for ranging sensor attacks on automotive systems

2022 · 2022 IEEE International Conference on Consumer Electronics (ICCE), 1-2, 2022 · 14 citations (GS)

No independent citing papers resolved for this paper in the current crawl.

FOLLOW-UP WORK

Automotive functional safety: Scope, standards, and perspectives on practice

2024 · IEEE Consumer Electronics Magazine 14 (1), 10-25, 2024 · 9 citations (GS)

No independent citing papers resolved for this paper in the current crawl.

FOLLOW-UP WORK

Vecaep: A hands-on exploration platform for vehicular communication attacks

2023 · 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 1-5, 2023 · 4 citations (GS)

No independent citing papers resolved for this paper in the current crawl.

D. Citing-Institution Prestige & Geography

Top citing institutions

Institution	Country	World ranking	Citing papers
University of Florida	United States	SCImago #166 · THE =134 · QS =212	9
Boston University	United States	SCImago #272 · THE =76 · QS =88	3
Massachusetts Institute of Technology	United States	SCImago #41 · THE 2 · QS 1	3
Tongji University	China	SCImago #82 · THE =141 · QS =177	2
Cyprus University of Technology	Cyprus	SCImago #5605 · THE 501–600 · QS =686	2
CSIRO Data61	—	—	2
New York University	United Arab Emirates	SCImago #116 · THE =31 · QS 55	2
University of Calgary	Canada	SCImago #399 · THE 200 · QS 211	2
University of Southampton	United Kingdom	SCImago #556 · THE 129 · QS 87	2
Arizona State University	United States	SCImago #357 · THE 201–250 · QS =173	2
University of Melbourne	Australia	SCImago #72 · THE 37 · QS 19	2
Texas A&M University	United States	THE =151 · QS 144	2
University of Michigan	United States	SCImago #43 · THE 23 · QS 45	2
Duke University	United States	SCImago #115 · THE 28 · QS 62	2
The University of Wollongong	Australia	SCImago #1289 · THE 201–250 · QS =184	1

Geographic distribution of citing authors

Country	Citing papers
United States	26
China	9
Australia	3
Cyprus	3
India	3
United Arab Emirates	3
United Kingdom	3
Canada	2
Iran	2
Luxembourg	1
Malaysia	1
Pakistan	1

Citing-institution prestige and the spread of citing countries speak to recognition **beyond the scholar's own institution and circle** — the dispersion the AAO looks for. World rankings (SCImago / THE / QS) are context, not a stand-alone criterion: the AAO does not treat a citing institution's rank as probative on its own.

F. AAO Precedent Considerations

Pre-filing self-check (AAO denial patterns)

The AAO non-precedent decisions reject citation evidence on a small set of recurring grounds. Confirm the petition addresses each before filing:

- ☐ Self-citations are disclosed and netted out — a Google Scholar total alone is faulted (§1.1).
- ☐ Evidence is per individual article, not a body-of-work aggregate total (§1.2).
- ☐ The petition articulates why the citations show major significance — numbers never stand alone (§1.5).
- ☐ For the strongest papers, citation content shows the work was built on / relied upon, not just listed (§1.6, §2.2).
- ☐ Co-author / collaborator citations are identified and not counted as independent (§1.7).
- ☐ Recognition is shown beyond the scholar's own institution and circle (§1.8).
- ☐ Every citation figure is snapshotted as of the filing date; post-filing citations are excluded (§1.9).
- ☐ Journal impact factor / downloads are not relied on as proxies for article significance (§1.10, §1.12).
- ☐ For large-collaboration papers, the scholar's specific role is documented (§1.13).
- ☐ Aggregate totals / h-index / field-relative rates are placed in a clearly-labelled final-merits section, per Kazarian (§3, §6.1.7).

Disclaimer

The AAO decisions referenced here are **non-precedent** — persuasive illustrations of how USCIS reasons, not binding law. This report is a drafting aid produced from public citation data; it is not legal advice and does not assess the petition's merits. All analysis must be reviewed by qualified immigration counsel.

G. Citation Evidence Index

Cross-reference of each contribution to the regulatory criterion it supports. Counsel should map these to the petition's exhibit numbers.

Contribution	Core paper	Indep. cites	Supports
Contribution 1	Security of emergent automotive systems: A tutorial introduction and perspectives on practice	27	8 CFR 204.5(i)(3) — Outstanding Researcher
Contribution 2	Redem: Real-time detection and mitigation of communication attacks in connected autonomous vehicle applications	6	8 CFR 204.5(i)(3) — Outstanding Researcher
Contribution 3	Autohal: An exploration platform for ranging sensor attacks on automotive systems	0	8 CFR 204.5(i)(3) — Outstanding Researcher