Citation Evidence Report

EB-1A Petition — Original Contributions of Major Significance

8 CFR § 204.5(h)(3)(v) · Criterion 5

Congyu Liu

Purdue University

Google Scholar profile

Generated 2026-05-21 by CiteMap. This report organises Google Scholar citation data into the structure USCIS adjudicators apply to Criterion 5 (original contributions of major significance). 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

92	106	5	5
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.

69.6% independent of 56 classified citing papers

Citation type	Count
Independent	39
Self-citation	2
Co-author	15
Same-institution	0

36 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 developed a testing framework for OS-level virtualization interference bugs and extended this work to transparent kernel-bypass networking, establishing a significant line of inquiry in system reliability and performance.

The researcher's contribution centers on a seminal 2023 paper titled 'Kit: Testing os-level virtualization for functional interference bugs,' which appears to introduce a method for identifying functional interference in virtualized environments. This core work is complemented by a 2025 follow-up, 'Pegasus: Transparent and unified kernel-bypass networking for fast local and remote communication,' suggesting a progression from system testing to high-performance networking solutions.

This line of work appears to address the challenge of ensuring reliability and performance in complex system architectures. The transition from testing virtualization bugs to developing transparent kernel-bypass networking indicates an original approach to mitigating interference while optimizing communication speeds, bridging the gap between system stability and network efficiency.

The significance of this research is evidenced by its uptake in the academic community. The core paper has garnered 23 citations, while the follow-up has received 12. Notably, 69.6% of the 56 classified citations originate from independent researchers, indicating that the work has resonated beyond the researcher's immediate circle and influenced broader scholarly discourse.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 13

CORE PAPER

Kit: Testing os-level virtualization for functional interference bugs

2023 · Proceedings of the 28th ACM International Conference on Architectural ..., 2023 · 23 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Unleashing unprivileged ebpf potential with dynamic sandboxing	University of British Columbia, Wake Forest University	Canada, United States	Background
2	Characterizing Trust Boundary Vulnerabilities in TEE Containers	Chinese Academy of Sciences, Duke University, Huazhong University of Science and Technology	China, Singapore, United States	—
3	CofferOS: Hardening OS-level Virtualization with Rust	FuriosaAI, KAIST, University of Illinois Urbana-Champaign	South Korea, United States	—
4	Comparing Isolation Mechanisms with OSmosis	University of British Columbia	Canada	—
5	Locked In, Leaked Out: Measuring Isolation via Kernel Locks	University of Wisconsin-Madison	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

Pegasus: Transparent and unified kernel-bypass networking for fast local and remote communication

2025 · Proceedings of the Twentieth European Conference on Computer Systems, 360-378, 2025 · 12 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	HypoVisor: Multi-Tenant POSIX Process Virtualization in Userspace for Untrusted Native Code	Oracle America, Inc.	United States	—
2	Opening Up {Kernel-Bypass}{TCP} Stacks	University of Edinburgh	United Kingdom	—
3	Not A DPU in Name Only! Unleashing RDMA-capable DPUs in Multi-Tenant Serverless Clouds with NADINO	Hewlett Packard, Hewlett Packard Enterprise, University of California, Riverside	United States	—
4	MorphOS: An Extensible Networked Operating System	Technical University of Munich	Germany	—
5	Joyride: Rethinking Linux's network stack design for better performance, security, and reliability	The Pennsylvania State University	United States	—
6	Libra: Accelerating Socket I/O via Programmable Selective Data Copying	Shanghai Jiao Tong University, University of Connecticut	China, United States	—
7	TransBridge: A Transparent Communication Middleware with Unified RoCE and TCP Semantics	National University of Defense Technology	China	—
8	STEER: Software Toolkit for Edge Efficient Retraining	Foundation for Research and Technology Hellas	Greece	—

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 2

Claim — Contribution 2

The researcher developed Veil, a protected services framework for confidential virtual machines, establishing a foundational approach to securing VM confidentiality.

The researcher's contribution centers on the development of Veil, a protected services framework for confidential virtual machines, as detailed in their 2023 publication. This work appears to address the critical need for robust confidentiality mechanisms within virtualized environments, offering a structured approach to protecting services in cloud and virtual infrastructure contexts.

By introducing a dedicated framework for confidential VMs, this line of work suggests a novel method for isolating and securing virtual machine operations. The absence of follow-up papers by the same researcher indicates that this single publication serves as the primary articulation of this specific architectural contribution, standing alone as a distinct technical proposal in the field.

The work has garnered significant attention, with 25 citations recorded. Notably, 69.6% of the citing papers originate from independent researchers, suggesting that the Veil framework has been adopted and built upon by the broader academic community rather than solely by the researcher's immediate collaborators. This high degree of independent uptake underscores the framework's relevance and utility to external scholars working on virtual machine security.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 12 · **1 flagged influential by Semantic Scholar**

CORE PAPER

Veil: A protected services framework for confidential virtual machines

2023 · Proceedings of the 28th ACM International Conference on Architectural ..., 2023 · 25 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	Dorami: Privilege Separating Security Monitor on {RISC-V}{TEEs}	ETH Zurich, Microsoft	Switzerland, United States	—
2	{CPC}: Flexible, Secure, and Efficient {CVM} Maintenance with Confidential Procedure Calls	Shanghai Jiao Tong University	China	—
3	{00SEVen}–Re-enabling Virtual Machine Forensics: Introspecting Confidential {VMs} Using Privileged {in-VM} Agents	CISPA Helmholtz Center for Information Security	Germany	—
4	{EKC}: A Portable and Extensible Kernel Compartment for {De-Privileging} Commodity {OS}	Shanghai Jiao Tong University, Shanghai Jiao Tong University, Southern University of Science and Technology, Southern University of Science and Technology	China	—
5	The road to trust: Building enclaves within confidential VMs	Chinese Academy of Sciences, Indiana University Bloomington, Institute of Information Engineering, CAS	China, United States	Background
6	Aster: Fixing the android tee ecosystem with arm cca	ETH Zurich	Switzerland	Background
7	Cabin: Confining Untrusted Programs within Confidential VMs	Chinese Academy of Sciences	China	**Methodology**
8	{TETD}: Trusted Execution in Trust Domains	Singapore Management University, Southern University of Science and Technology	China, Singapore	—
9	NanoZone: Scalable, Efficient, and Secure Memory Protection for Arm CCA	George Mason University, Huazhong University of Science and Technology	China, P. R. China, United States	—
10	SKernel: An Elastic and Efficient Secure Container System at Scale with a Split-Kernel Architecture	Ant Group, Shanghai Jiao Tong University, Tsinghua University	China	—
11	Rethinking the confidential cloud through a unified low-level abstraction for composable isolation	EPFL, Imperial College London, Microsoft	Switzerland, United Kingdom, United States	**Influential**
12	TESLA: Trusted Execution Support for Legacy Embedded Applications	Incore Semiconductors Pvt. Ltd., Indian Institute of Technology Madras	India	—

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 Cabin: Confining Untrusted Programs within Confidential VMs

"To accommodate other frameworks like Veil [9], Cabin require at least one VMPL lower than the guest OS."

Contribution 3

Claim — Contribution 3

The researcher developed Pardiff, a practical static differential analysis framework for network protocol parsers, establishing a novel approach to identifying parsing discrepancies and potential vulnerabilities.

The researcher's contribution centers on the development of Pardiff, introduced in a 2024 paper titled 'Pardiff: Practical static differential analysis of network protocol parsers.' This work represents a focused effort to apply static differential analysis techniques specifically to the domain of network protocol parsing, aiming to improve the detection of inconsistencies and security flaws in parser implementations.

This line of work appears to address the challenge of verifying the correctness and security of network protocol parsers, which are critical infrastructure components often prone to subtle implementation errors. By proposing a 'practical' static differential analysis method, the researcher suggests a shift toward more scalable and applicable verification techniques compared to prior approaches, filling a gap in automated security analysis for network software.

The significance of this contribution is evidenced by its rapid uptake in the academic community, with 15 citations recorded since its 2024 publication. Notably, the broader citation context for this scholar indicates that 69.6% of citing works originate from independent researchers, suggesting that the methodology or findings have resonated beyond the immediate research group and are being adopted by external parties in the field.

INDEPENDENT CITATIONS FOR THIS CONTRIBUTION: 4

CORE PAPER

Pardiff: Practical static differential analysis of network protocol parsers

2024 · Proceedings of the ACM on Programming Languages 8 (OOPSLA1), 1208-1234, 2024 · 15 citations (GS)

No.	Citing paper	Citing institution(s)	Country	S2
1	A survey of protocol fuzzing	Nanjing University, Nanyang Technological University, Singapore Management University	Australia, China, Singapore	—
2	Toss a Fault to BpfChecker: Revealing Implementation Flaws for eBPF runtimes with Differential Fuzzing	The Hong Kong Polytechnic University, Zhejiang University	China	—
3	3dgen: Ai-assisted generation of provably correct binary format parsers	Microsoft Research	United States	—
4	Validating Interior Gateway Routing Protocols via Equivalent Topology Synthesis	Nanjing University	China	—

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).

D. Citing-Institution Prestige & Geography

Top citing institutions

Institution	Country	World ranking	Citing papers
Purdue University	United States	SCImago #255 · QS =88	14
Shanghai Jiao Tong University	China	SCImago #10 · THE 40 · QS =47	5
Chinese Academy of Sciences	China	SCImago #2	4

Institution	Country	World ranking	Citing papers
Nanjing University	China	SCImago #178 · THE =62 · QS =103	3
Intel	United States	—	3
Google DeepMind	United States	SCImago #90	2
Arizona State University	United States	SCImago #357 · THE 201–250 · QS =173	2
Texas A&M University	United States	THE =151 · QS 144	2
Huazhong University of Science and Technology	P. R. China	SCImago #25 · THE =176 · QS 319	2
Indiana University Bloomington	United States	SCImago #798 · QS =306	2
George Mason University	United States	SCImago #1399 · THE 401–500 · QS 951-1000	2
Zhejiang University	China	SCImago #6 · THE 39 · QS 49	2
Microsoft	United States	—	2
Nanyang Technological University	Singapore	SCImago #137	2
ETH Zurich	Switzerland	THE 11 · QS 7	2

Geographic distribution of citing authors

Country	Citing papers
United States	31
China	19
Germany	5
Singapore	4
South Korea	3
Canada	3
Switzerland	3
United Kingdom	3
Japan	1
Belgium	1
Greece	1
India	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	Kit: Testing os-level virtualization for functional interference bugs	13	8 CFR 204.5(h)(3)(v) — Criterion 5
Contribution 2	Veil: A protected services framework for confidential virtual machines	12	8 CFR 204.5(h)(3)(v) — Criterion 5
Contribution 3	Pardiff: Practical static differential analysis of network protocol parsers	4	8 CFR 204.5(h)(3)(v) — Criterion 5