Sumit Kumar Jha

Professor of Computer & Information Science & Engineering • University of Florida

U.S. Citizen

EDUCATION

CARNEGIE MELLON UNIVERSITY
Ph.D., Computer Science
2010

CARNEGIE MELLON UNIVERSITY
M.S., Computer Science
2009

IIT KHARAGPUR
B.Tech. (Honors), Computer Science & Engineering
2004

sumit.jha@ufl.edu • sumitkumarjha.com • Google Scholar • DBLP • ORCID 0000-0003-0354-2940

RESEARCH PROFILE

Sumit Kumar Jha works on **formal methods and trustworthy AI**: verification and synthesis techniques that make learned systems interpretable, controllable, and certifiable. One line of work develops neuro-symbolic methods that hold machine learning to logical specifications, including counterexample-guided synthesis with LLMs, temporal-logic grounding of natural language, formal verification of chain-of-thought faithfulness, and contract enforcement over multi-agent trajectories. A second develops attribution and steering methods for inspecting and controlling model internals. Both now apply to AI for science: scientific foundation models and formal analysis of their internal representations.

He earned his Ph.D. in Computer Science from Carnegie Mellon University, held the AFOSR Young Investigator Program award, and completed four visiting appointments at AFRL. He has served as lead or prime PI on DARPA CLARA, GARD, TIAMAT, and UPTAIC awards, NSF SPX and SHF awards, and a DOE ASCR multi-institution project, as UF node PI on DARPA AutoDIDACTS and the Argonne-led DOE MAESTRO project, with additional support from ONR, AFRL/AFOSR, and national laboratories including Oak Ridge, including export-controlled (ITAR) work for NGA. His work appears at AAAI, ACL, CVPR, DAC, EMNLP, HSCC, ICLR, ICML, IJCAI, and NeurIPS, and in IEEE Transactions journals and TMLR.

VISITING APPOINTMENTS

Summer 2020	**Air Force Research Laboratory**, AFOSR Summer Faculty Fellowship
Summer 2018	**Air Force Research Laboratory**, Visiting Faculty Research Program
Summer 2014	**Air Force Research Laboratory**, AFOSR Summer Faculty Fellowship
Summer 2013	**Air Force Research Laboratory**, Visiting Faculty Research Program
Summer 2006	**Microsoft Research**, Bangalore, India
Summer 2005	**General Motors R&D**, Warren, MI
Summer 2003	**INRIA**, Nancy, France

SELECTED PUBLICATIONS

Career-spanning selection in formal methods and trustworthy AI. Bibliometrics (Google Scholar, July 2026): **3,179** citations • **h-index 29** • **i10-index 62**. Full list of 180 publications available on request.

1. V. Pramanik, M. Maliha, O. Kotevska, N.D. Bastian, S. Jha, **S.K. Jha**. *Harmless in Pieces, Harmful in Motion: Detecting Multi-Agent Jailbreaks*. NeurIPS, 2026.
2. V. Pramanik, M. Maliha, O. Kotevska, A. Ramanathan, N.D. Bastian, S. Jha, **S.K. Jha**. *Unified Resource-Grounded Coordination Protocol for Orchestrator-Free Heterogeneous Multi-Agent Systems*. NeurIPS, 2026.
3. M. Maliha, V. Pramanik, **S.K. Jha**. *ATC: Agent Trajectory Control for Role-Contract Enforcement in Black-Box Multi-Agent Systems*. EMNLP (Main Conference, Oral), 2026.
4. V. Pramanik, M. Maliha, S. Jha, **S.K. Jha**. *Drift No More: Spectral Locking for Long-Horizon Open-Weight Multi-Agent AI*. EMNLP (Main Conference), 2026.

5. V. Pramanik, M. Maliha, N.D. Bastian, A. Velasquez, S. Jha, **S.K. Jha**. *NSF-CoT: Neuro-Symbolic Formal Verification of Chain-of-Thought Faithfulness*. ACL Findings, 2026.
6. V. Pramanik, M. Maliha, N.D. Bastian, **S.K. Jha**. *Hessian-Enhanced Token Attribution (HETA): Interpreting Autoregressive Language Models*. ICLR, 2026.
7. V. Pramanik, M. Maliha, S. Jha, **S.K. Jha**. *Jailbreaking the Matrix: Nullspace Steering for Controlled Model Subversion*. ICLR, 2026.
8. W.H. English, D. Simon, **S.K. Jha**, R. Ewetz. *Grammar-Forced Translation of Natural Language to Temporal Logic using LLMs*. ICML, 2025.
9. **S.K. Jha**, S. Jha, P. Lincoln, N.D. Bastian, A. Velasquez, R. Ewetz, S. Neema. *Counterexample-Guided Inductive Synthesis using Large Language Models and Satisfiability Solving*. MILCOM, 2023.
10. **S.K. Jha**, R. Ewetz, A. Velasquez, A. Ramanathan, S. Jha. *Shaping Noise for Robust Attributions in Neural Stochastic Differential Equations*. AAAI, 2022.
11. S. Jha, S. Raj, S.L. Fernandes, **S.K. Jha**, S. Jha, B. Jalaian, G. Verma, A. Swami. *Attribution-Based Confidence Metric for Deep Neural Networks*. NeurIPS, 2019.
12. S. Jha, S. Raj, **S.K. Jha**, N. Shankar. *Duality-Based Nested Controller Synthesis from STL Specifications for Stochastic Linear Systems*. FORMATS, 2018.
13. **S.K. Jha**, E.M. Clarke, C.J. Langmead, A. Legay, A. Platzer, P. Zuliani. *A Bayesian Approach to Model Checking Biological Systems*. CMSB, 2009.
14. **S.K. Jha**, B.H. Krogh, J.E. Weimer, E.M. Clarke. *Reachability for Linear Hybrid Automata using Iterative Relaxation Abstraction*. HSCC, 2007.

FUNDED RESEARCH

ACTIVE

1. **PRAGMA: Proof-Refined Argumentation-Grounded AR-ML Architecture.** DARPA DSO, CLARA program. PI.
2. **FLARE: Foundational Laws & Automated Rule Extraction for Detonation-Ready Injector Design.** DARPA AutoDIDACTS. Selected; PI of the UF node.
3. **MAESTRO: Modular Autonomous Experimentation through Self-improving Testbeds for Robotic Operations.** DOE ASCR, Argonne-led. Selected; PI of the UF node.
4. **Research in Scalable, Privacy-Preserving Machine Learning Within Federated Learning.** DOE / ORNL. PI.
5. **AI-CRAFT: Artificial Intelligence Cybersecurity Readiness & Future Training.** DARPA UPTAIC program. PI.
6. **FMitF: Synthesis & Verification of In-Memory Computing Systems using Formal Methods.** NSF. PI of his node.

COMPLETED

7. **FIRST-FM: Few-shot In-context Learning for Robust Semantic Transfer.** DARPA TIAMAT program. PI. 2024–2026.
8. **INSTA-AI / NSAR: Neural Representations & their Symbolic Twins for Assured AI.** DARPA ANSR program, via AFRL/UCF cooperative agreement. PI of the subaward. 2023–2026.
9. **MEDAL: Mobilizing Emerging AI Talent through Autonomous Scientific Laboratories.** DOE Office of Advanced Scientific Computing Research. Lead PI, six institutions including Argonne National Laboratory. 2023–2026.
10. **AFRL ML-RCP II.** Three projects under the Ohio State University prime cooperative agreement: BRAIN-Code, RL-CAP, and PolySAT. PI. 2025.
11. **ALARM: Attributions & Learning Dynamics based Adaptive Defense & Robustness Metric.** DARPA GARD program, HR00112020002. Prime PI at award. 2020–2024.
12. **SPX: Automated Synthesis of Extreme-Scale Computing Systems using Non-Volatile Memory** (2018–2023) and **XPS: Formal-Methods-Based Algorithmic Synthesis of More-than-Moore Nano-Crossbars** (2014–2017). NSF. Lead PI of both, each a two-node collaborative with SUNY Polytechnic.
13. **SHF: Exascale Formal Verification Algorithms for Parameterized Probabilistic Models.** NSF. PI. 2014–2019.
14. **FASTER: Formal-Methods-Based Synthesis of Stochastic In-Exact In-Memory Computing.** AFOSR Young Investigator Program. PI. 2016–2019.
15. **PANDA: Predictive Maintenance using Neural ODEs, Deep Koopman & Attribution Analysis.** ONR Science of AI. PI. 2020–2023.
16. **Explainable High-Confidence Models for Dynamical Systems** (DOE NNSA / Oak Ridge National Laboratory, PI, 2021–2023) and **Robust Explanations via Adversarially Trained Ensembles & Attribution-based Confidence** (DOE EXPRESS, PI of the FIU subaward, 2022–2024).
17. **SaTC-EDU: Integrating Cybersecurity in Computing Curricula.** NSF. Originating PI. 2023.
18. **Adversarial Fingerprints & Robust Fingerprint Detection** (three awards). Royal Bank of Canada; Florida High-

Tech Corridor Council. PI. 2015–2020.

HONORS & AWARDS

- **Air Force Young Investigator Program Award**, AFOSR (2016). **Eminent Scholar Chair Professor**, FIU (2024); **FIU Top Scholar Award** (2025); UTSA Research Achievement Award university nomination (2023).
- **Best Paper Awards**: FPS 2018; IEEE ICCABS 2014, 2011. **Best Paper Nominations**: MILCOM 2023; ICCAD 2022; DATE 2021; AISafety@IJCAI 2019. CVPR 2026 Highlight Paper.
- **Fellowships**: US Air Force Summer Faculty Fellowship, AFOSR (2014, 2020); AFRL Visiting Faculty Research Program (2013, 2018); UCF Predictive Analytics Innovation Fellow (2017); CMU SCS Graduate Fellowship (2004–2010). IEEE Orlando Section Outstanding Engineering Educator Award (2013); Elected Full Member, Sigma Xi (2012); Top Reviewer, NeurIPS (2025); Top Area Chair recognition, NeurIPS (2026); Outstanding TPC Member, DAC 2026. Senior Member, IEEE.

PATENTS & TECHNOLOGY TRANSFER

- *System & Method for Path-Based In-Memory Computing*, US App. 2024/0311038 A1 (2024, pending), UCF Research Foundation & UT System • *3-D Crossbar Architecture for In-Memory Computing of Graph Transitive Closure*, US 11,538,989 B2 (2022), UCF • *Computation of Boolean Formulas using Sneak Paths in Crossbar Computing*, US 9,319,047 B2 (2016), UCF / U.S. Air Force.
- *Systems & Methods for Dynamic Passphrases*, US 11,429,712 (2022), US 11,893,099 (2024), and continuation US 12,306,919 (2025), Royal Bank of Canada • *Stochastic Computational Model Parameter Synthesis System*, US 9,558,300 B2 (2017), Carnegie Mellon University & UCF Research Foundation • *Object Relational Map Verification System*, US 7,702,695 B2 (2010), Microsoft Corporation.

MERIT REVIEW, PANEL & PROGRAM SERVICE

- **Reviewer / Panelist, National Science Foundation**, eleven consecutive years (2016–2026), across formal methods, trustworthy AI, and security programs. Also reviewer for DOE (2020, 2022–2026), AFOSR (2016, 2017), U.S. Army Research Laboratory (2023), the Swiss NSF (2018), and the Texas Higher Education Coordinating Board (2021).
- **External evaluator** for faculty promotion (Vanderbilt, 2026) and research-staff promotion (Oak Ridge National Laboratory, 2026). Regular participant in DARPA, ONR Science of AI, and DOE/ASCR PI meetings (2020–2026).
- **Conference leadership**: Area Chair, NeurIPS 2026; Program Track Chair, IEEE ISQED 2026 and IEEE ICCD 2022; Track Co-Chair, ISQED 2024, 2025; Program Chair, IEEE ICCABS 2020. **Program committees**: AAAI (2023–2027), NeurIPS (2023–2026), ICML (2025, 2026), ICLR (2024–2026), CVPR (2022, 2026), ECCV (2026), ACL/ARR (2026), VMCAI (2025), DAC (2026), ICCAD (2024–2026).
- **Bridge Program, AAAI-27** (Montréal, February 16–17, 2027): proposal "Systems That Keep Changing: Trust, Provenance, and Safety in Autonomous Science" accepted.
- **University governance**: Post-Tenure Review Committee, College of Engineering, UF (2026); elected Faculty Senator at FIU (2024) and UCF (2020); chair or co-chair of CS faculty searches at UTSA and FIU.

STUDENTS & MENTORING

- **11 Ph.D. students graduated** (2016–2024), placed into faculty positions, national laboratories, government, and industry, including **Alvaro Velasquez** (AFRL; Asst. Prof., CU Boulder), Dwaipayan Chakraborty (ORNL; Rowan University), Sunny Raj (Oakland University), and Faraz Hussain (Clarkson University).
- **5 postdoctoral researchers** mentored (2020–2025), four now in faculty roles; **6 M.S. thesis students** graduated; service on **13 Ph.D. dissertation committees** (2012–2023); **33 undergraduate researchers** mentored (2011–2026), including NSF REU and Office of Undergraduate Research awardees.
- **Mentee honors**: NSF Graduate Research Fellowships (A. Velasquez, 2015; E. Sassano, 2012); UCF Outstanding Thesis Award and "30 under 30" (A. Velasquez); UCF ORC Fellowship (S. Thijssen, 2020); UF Emerging Scholars Program (T. Raj, 2026).
- Created and taught a graduate *Trust in AI* course; Graduate Advisor of Record, MS in CS and MS in AI, UTSA (2021–2023).

CURRENT PH.D. STUDENTS, UNIVERSITY OF FLORIDA

Vishal Pramanik (M.S., IIT Bombay)
Brian Rodriguez (M.S., FIU)
Brandon Rodriguez (M.S., FIU)
Abigail Lin (B.S., UF)
Kexin Zhou (B.S., UF)
Abdur Rahman Shibly (B.S., BUET)
Mahmudul Hasan (B.S., BUET)
Praveena Simhadri (B.S., IIT Kharagpur)