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

PROFILE

Sumit Kumar Jha is a Professor of Computer & Information Science & Engineering at the University of Florida and a U.S. citizen. He earned his Ph.D. in Computer Science from Carnegie Mellon University, held the AFOSR Young Investigator Program award, and completed multiple visiting appointments at the Air Force Research Laboratory. His research focuses on formal methods, interpretable controllable AI, and the automated synthesis of AI systems. His current interests center on AI for science: agentic AI, scientific foundation models, and the formal analysis of their internal representations. He has served as lead/prime PI on DARPA GARD (ALARM), DARPA TIAMAT (FIRST-FM), NSF SPX, DOE ASCR MEDAL, and DARPA AI-CRAFT, with additional support from NSF, DOE, ONR, and AFRL/AFOSR, including export-controlled (ITAR) projects for the National Geospatial-Intelligence Agency (NGA) and AFRL subawards. His work appears at AAAI, ACL, CVPR, DAC, ICCAD, ICLR, ICML, IJCAI, and NeurIPS, and in IEEE Transactions journals and TMLR.

ACADEMIC APPOINTMENTS

2025–present	**Professor**, Computer & Information Science & Engineering, University of Florida
2024–2025	**Eminent Scholar Chair Professor**, Florida International University
2023–2025	**Professor**, Computer Science, Florida International University
2020–2023	**Professor**, Computer Science, University of Texas at San Antonio
2016–2020	**Associate Professor**, Computer Science, University of Central Florida
2010–2016	**Assistant Professor**, Computer Science, University of Central Florida

VISITING & SUMMER 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 **Institut National de Recherche en Informatique et en Automatique (INRIA)**, Nancy, France

SELECTED PUBLICATIONS

Bibliometrics (Google Scholar, June 2026): **3,058** citations • **h-index 28** • **i10-index 60** (since 2021: 1,658 / 21 / 45). The complete publication list appears at the end of this document.

1. 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. PDF
2. V. Pramanik, M. Maliha, S. Jha, A. Velasquez, O. Kotevska, **S.K. Jha**. *Selective Amnesia: Contrastive Subnet Erasure for Class-Level Unlearning in Vision Models*. CVPR (Highlight Paper), 2026. PDF
3. V. Pramanik, M. Maliha, N.D. Bastian, **S.K. Jha**. *Hessian-Enhanced Token Attribution (HETA): Interpreting Autoregressive Language Models*. ICLR, 2026. arXiv
4. V. Pramanik, M. Maliha, S. Jha, **S.K. Jha**. *Jailbreaking the Matrix: Nullspace Steering for Controlled Model Subversion*. ICLR, 2026. arXiv
5. P. Nwaorgu, S. Singireddy, A. Beckus, A. McKinney, M. Alinejad, C. Enyioha, **S.K. Jha**, A. Velasquez, G.K. Atia. *Automaton Distillation: Neuro-Symbolic Transfer Learning for Deep RL*. TMLR, 2026. PDF
6. W.H. English, D. Simon, **S.K. Jha**, R. Ewetz. *Grammar-Forced Translation of Natural Language to Temporal Logic using LLMs*. ICML, 2025. PMLR
7. C. Walker, **S.K. Jha**, R. Ewetz. *Metric-Driven Attributions for Vision Transformers*. ICLR, 2025. OpenReview
8. C. Walker, R. Ahmed, **S.K. Jha**, R. Ewetz. *Explaining ViTs Using Information Flow*. AISTATS, 2025. PMLR
9. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, R. Ewetz. *LOGIC: Logic Synthesis for Digital In-Memory Computing*. ACM TODAES, 2025. doi
10. I. Alkhouri, **S.K. Jha**, A. Beckus, G. Atia, S. Jha, R. Ewetz, A. Velasquez. *Exploring the Predictive Capabilities of AlphaFold Using Adversarial Protein Sequences*. IEEE TAI, 2024. doi
11. S. Thijssen, M. Rashed, **S.K. Jha**, R. Ewetz. *PATH: Evaluation of Boolean Logic using Path-based In-Memory Computing Systems*. IEEE TCAD, 2024. doi
12. C. Walker, **S.K. Jha**, K. Chen, R. Ewetz. *Integrated Decision Gradients: Compute Your Attributions Where the Model Makes Its Decision*. AAAI, 2024. doi
13. S. Thijssen, M. Rashed, R. Ahmed, S. Singireddy, **S.K. Jha**, R. Ewetz. *Equivalence Checking for Flow-Based Computing using Iterative SAT Solving*. ICCAD, 2024. doi
14. **S.K. Jha**, S. Jha, R. Ewetz, A. Velasquez. *On the Design of a Novel Attention Mechanism for Enhanced Efficiency of Transformers*. DAC, 2024. doi
15. S. Thijssen, M. Rashed, **S.K. Jha**, R. Ewetz. *Synthesis of Compact Flow-based Computing Circuits from Boolean Expressions*. DAC, 2024. doi
16. M. Rashed, S. Thijssen, D. Simon, **S.K. Jha**, R. Ewetz. *Execution Sequence Optimization for Processing In-Memory using Parallel Data Preparation*. DAC, 2024. doi
17. K. Kumari, M. Jadliwala, **S.K. Jha**, A. Maiti. *Game-Theoretic Understanding of Explanation-Based Membership Inference Attacks*. GameSec, 2024. doi
18. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, F. Yao, R. Ewetz. *STREAM: Toward READ-Based In-Memory Computing for Streaming-Based Data-Intensive Applications*. IEEE TCAD, 2023. doi
19. S. Thijssen, M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *UpTime: Towards Flow-based In-Memory Computing with High Fault-Tolerance*. DAC, 2023. doi

20. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, R. Ewetz. *Automated Synthesis for In-Memory Computing*. ICCAD, 2023. doi
21. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, H. Zheng, R. Ewetz. *Path-Based Processing using In-Memory Systolic Arrays for Accelerating Data-Intensive Applications*. ICCAD, 2023. doi
22. S. Thijssen, M. Rashed, **S.K. Jha**, R. Ewetz. *Verification of Flow-Based Computing Systems Using Bounded Model Checking*. ICCAD, 2023. doi
23. S. Jha, **S.K. Jha**, P. Lincoln, N.D. Bastian, A. Velasquez, S. Neema. *Dehallucinating Large Language Models using Formal-Methods-Guided Iterative Prompting*. IEEE ICAA, 2023. doi
24. N. Uysal, B. Zhang, **S.K. Jha**, R. Ewetz. *XMAP: Programming Memristor Crossbars for Analog Matrix-Vector Multiplication*. IEEE TCAD, 2022. doi
25. S. Thijssen, **S.K. Jha**, R. Ewetz. *COMPACT: Flow-Based Computing on Nanoscale Crossbars with Minimal Semiperimeter and Maximum Dimension*. IEEE TCAD, 2022. doi
26. **S.K. Jha**, R. Ewetz, A. Velasquez, A. Ramanathan, S. Jha. *Shaping Noise for Robust Attributions in Neural Stochastic Differential Equations*. AAAI, 2022. doi
27. M.R.H. Rashed, A. Awad, **S.K. Jha**, R. Ewetz. *Towards Resilient Analog In-Memory Deep Learning via Data Layout Re-Organization*. DAC, 2022. doi
28. S. Thijssen, **S.K. Jha**, R. Ewetz. *PATH: Evaluation of Boolean Logic Using Path-Based In-Memory Computing*. DAC, 2022. doi
29. M.R.H. Rashed, **S.K. Jha**, F. Yao, R. Ewetz. *Hybrid Digital-Digital In-Memory Computing*. DATE, 2022. doi
30. M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *Logic Synthesis for Digital In-Memory Computing*. ICCAD, 2022. Best Paper Nominee. doi
31. **S.K. Jha**, A. Velasquez, R. Ewetz, L. Pullum, S. Jha. *ExplainIt!: A Tool for Computing Robust Attributions of DNNs*. IJCAI, 2022. doi
32. S. Rafiq, J. Hazra, M. Liehr, K. Beckmann, M. Abedin, J.S. Pannu, **S.K. Jha**, N.C. Cady. *Investigation of ReRAM Variability on Flow-Based Edge Detection Computing Using HfO2-Based ReRAM Arrays*. IEEE TCAS-I, 2021. doi
33. S. Thijssen, **S.K. Jha**, R. Ewetz. *COMPACT: Flow-Based Computing on Nanoscale Crossbars with Minimal Semiperimeter*. DATE, 2021. Best Paper Nominee. doi
34. M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *Hybrid Analog-Digital In-Memory Computing*. ICCAD, 2021. doi
35. **S.K. Jha**, R. Ewetz, A. Velasquez, S. Jha. *On Smoother Attributions using Neural Stochastic Differential Equations*. IJCAI, 2021. doi
36. J.S. Pannu, S. Raj, S.L. Fernandes, D. Chakraborty, S. Rafiq, N.C. Cady, **S.K. Jha**. *Design and Fabrication of Flow-Based Edge Detection Memristor Crossbar Circuits*. IEEE TCAS-II, 2020. doi
37. 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. proc.
38. E.M. Clarke, A. Fehnker, **S.K. Jha**, H. Veith. *Temporal Logic Model Checking* (book chapter). Handbook of Networked & Embedded Control Systems, Springer, 2005. doi

FUNDED RESEARCH | NSF AWARDS

- **FMitF: Synthesis & Verification of In-Memory Computing Systems using Formal Methods** (Formal Methods in the Field). PI of his node; node share $250,000 of a $750,000 collaborative with R. Ewetz and N. Cady/SUNY. Award chain: #2319401 (UTSA) → #2404036 (FIU) → #2610233 (UF, 2025–2027).
- **SPX: Automated Synthesis of Extreme-Scale Computing Systems using Non-Volatile Memory**. Lead PI of an approximately $1M collaborative: node share $500,000 (#1822976, UCF, 2018; transferred to UTSA #2113307 and FIU #2408925) and $500,000 for the partner node led by N. Cady (#1823015, SUNY Polytechnic).

- **SaTC-EDU: Integrating Cybersecurity in Computing Curricula: Identity & Access Management** (SaTC). Originating PI (UTSA); subsequent PI of record T. Korkmaz. $100,001. #2302615.
- **XPS: Formal-Methods-Based Algorithmic Synthesis of More-than-Moore Nano-Crossbars**. Lead PI of an approximately $300,000 collaborative: node share $215,035 (UCF, #1438989) and $84,896 for the partner node led by N. Cady (#1438987, SUNY Polytechnic). 2014–2017.
- **SHF: Exascale Formal Verification Algorithms for Parameterized Probabilistic Models**. PI; $503,627. #1422257. 2014–2019.

FUNDED RESEARCH | FEDERAL & INDUSTRY

Figures follow the customary convention of stating the total award value at the prime institution (inclusive of administered subawards), the full value of a collaborative award at the lead institution, or the total value of a multi-institution project, as noted. Defense and DOE projects may be administered as cooperative agreements, OTAs, or subawards.

- **MEDAL: Mobilizing Emerging AI Talent through Autonomous Scientific Laboratories.** DOE ASCR. Lead PI of a multi-institution project spanning six institutions including Argonne National Laboratory; project total approximately $5.1M. 2023–2026 (FIU).
- **AI-CRAFT: Artificial Intelligence Cybersecurity Readiness & Future Training.** DARPA UPTAIC program, cooperative agreement HR00112420004. PI; $4,499,555 prime award at FIU (2023–2026), directing subawards to West Virginia University and Marshall University; work continues at UF under subaward.
- **INSTA-AI / NSAR: Neural Representations & their Symbolic Twins for Assured AI.** DARPA ANSR program; UCF prime cooperative agreement FA8750-23-2-0501, PI H. Zheng. PI/subawardee; $990,797 planned subaward at time of award, partially realized as FIU and UF subawards. 2023–2027.
- **FIRST-FM: Few-shot In-context Learning for Robust Semantic Transfer.** DARPA TIAMAT program, prototype OTA HR00112490420. PI; two-phase award totaling $1.98M (2024–2027); continues at UF under subaward.
- **ALARM: Attributions & Learning Dynamics based Adaptive Defense & Robustness Metric.** DARPA GARD program, cooperative agreement HR00112020002. PI; approximately $973K. 2020–2024.
- **AFRL ML-RCP II.** Three funded projects under the Ohio State University prime cooperative agreement: BRAIN-Code (neuro-symbolic code assurance for LLMs), $200,000; RL-CAP (explaining reinforcement learning via logic, automata & program synthesis), $140,000; PolySAT (polyglot synthesis via SAT), $82,400. PI; awarded 2025.
- **PANDA: Predictive Maintenance using Neural ODEs, Deep Koopman & Attribution Analysis.** ONR Science of AI. PI; approximately $262,200. 2020–2023.
- **Robust Explanations via Adversarially Trained Ensembles & Attribution-based Confidence.** DOE EXPRESS program; $400,000 total, UCF lead (R. Ewetz). PI of the FIU subaward ($160,000). 2022–2024.
- **FASTER: Formal-Methods-Based Synthesis of Stochastic In-Exact In-Memory Computing.** AFOSR Young Investigator Program. PI; approximately $300,000. 2016–2019.
- **Explainable High-Confidence Models for Dynamical Systems.** DOE National Nuclear Security Administration / Oak Ridge National Laboratory. PI; $200,000. 2021–2023.
- **Algorithmic Validation via Information-Theoretic Measures & Bayesian Statistics.** UT-Battelle / Oak Ridge National Laboratory. PI; $99,994. 2015.
- **Adversarial Fingerprints & Robust Fingerprint Detection (Facial-Recognition & Patterns-of-Life Extensions).** Royal Bank of Canada. PI; $155,249. 2019–2021.
- **Adversarial Fingerprints & Robust Fingerprint Detection.** Royal Bank of Canada. PI; $49,657. 2018–

2019.

- **Cybersecurity for Mobile-Banking Platforms.** Royal Bank of Canada. PI; $50,067. 2015–2016.
- **Adversarial-Fingerprint Synthesis & Facial-Recognition Extensions.** Florida High-Tech Corridor Council. PI; $51,747. 2019–2020.
- **Collaborative Cybersecurity Research at Florida SUS Institutions.** Florida Center for Cybersecurity (CyberFlorida). Lead PI; $74,838. 2018–2019.

FUNDED RESEARCH AT THE UNIVERSITY OF FLORIDA

Fetched from University of Florida award records (June 2026): four funded awards, $1,498,036 released to date. Several are collaborative subawards on which the candidate serves as a performer or institutional-node PI.

- **AI-CRAFT: Artificial Intelligence Cybersecurity Readiness and Future Training.** UF award AWD19968; PD/PI. Sponsor: Florida International University, Subaward #001075; prime sponsor: DARPA, HR0011-24-2-0004. $799,979 authorized; 02/20/2026–12/31/2026.
- **FIRST-FM: Few-shot In-context Learning for Robust Semantic Transfer using Multi-modal Foundation Models and Formal Methods.** UF award AWD19617; PD/PI. Sponsor: Florida International University, Subaward #001074; prime sponsor: DARPA, HR0011-24-9-0420 (prototype OTA). $319,751 authorized of $817,808 total anticipated; 08/15/2025–04/30/2026.
- **Collaborative Research: FMitF Track I: Synthesis and Verification of In-Memory Computing Systems using Formal Methods.** UF award AWD20087; PD/PI. Sponsor: National Science Foundation, #2610233. $197,273 authorized; 10/01/2025–08/31/2027.
- **INSTA-AI / NSAR: Integrating Neural Representation and their Symbolic Twins for Assured AI.** UF award AWD19603; PD/PI. Sponsor: University of Central Florida, GR108163-2; prime sponsor: U.S. Air Force Research Laboratory (DARPA ANSR program), FA8750-23-2-0501. $181,033 authorized; 09/01/2025–06/30/2026.

RESEARCH ADMINISTRATION, LEADERSHIP & PROGRAM SERVICE

MERIT REVIEW & PANEL SERVICE

- Reviewer / Panelist, National Science Foundation: eleven consecutive years (2016–2026), including ad hoc review for the NSF CAREER program; service across programs in formal methods, trustworthy/assured AI, and security.
- Reviewer, Department of Energy (2020, 2022–2026); AFOSR (2016, 2017); U.S. Army Research Laboratory (2023); Swiss National Science Foundation (2018); Texas Higher Education Coordinating Board OER program (2021).
- Regular participant in DARPA, ONR Science of AI, and DOE/DOE-ASCR PI meetings and agency workshops (2020–2026).

CONFERENCE LEADERSHIP & PROGRAM COMMITTEES

- Program Track Chair, IEEE ISQED 2026, and Program Track Co-Chair, IEEE ISQED 2025 and 2024 (Design, Test & Verification). Area Chair, NeurIPS 2026. Program Track Chair, IEEE ICCD 2022; Program Chair, IEEE ICCABS 2020.
- Program committees & reviewing: AAAI (2023–2026); NeurIPS (2023–2025, incl. Datasets & Benchmarks track); ICML (2025; Position-Paper Track 2026); ICLR (2024, 2025); CVPR (2022, 2026); ECCV (2026); ACL/ARR (2026); ECAI (2025); VMCAI (2025); Neuro-Symbolic Systems (NeuS, 2026); DAC (2026); ICCAD (2024–2026); ICCD (2023). Workshop program committees include ICCV U&ME (2025), CVPR MUV (2026), and ICLR Trustworthy AI (2026).

UNIVERSITY GOVERNANCE & ACADEMIC ADMINISTRATION

- Post-Tenure Review (PTR) Committee, College of Engineering, University of Florida (2026); proxy departmental representative, Promotion & Tenure Committee, University of Florida (2026).
- Elected Faculty Senator – Florida International University (2024) and University of Central Florida (2020).
- Co-Chair, Faculty Search Committee, FIU (2024); Chair of three CS faculty searches at UTSA (Data-Driven Intelligence, Cybersecurity, Systems; 2022); member, CS faculty search committees, UCF (2015, 2016, 2018) and Big Data search, Mathematics Department (2015).
- University Faculty Awards Selection Committee (2022) and CS Academic Review Committee (2020), UTSA; College of Engineering & Computer Science representative, University Admissions & Standards Committee, UCF (2014).
- Graduate Advisor of Record / Graduate Chair, MS in CS (2021–2023) and MS in AI (2022–2023), UTSA; Founding Co-Director, FinTech Program, UCF (2019–2020).
- Chair, IEEE Computer Society Orlando Chapter (2014, 2015).

SELECTED HONORS & AWARDS

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

TEACHING, MENTORING & EDUCATION

- Created and taught a graduate *Trust in AI* course (approximately 50 students, 2020–2024); created graduate independent studies on Automated Synthesis and Satisfiability Solving (2017–2020); Founding Co-Director, UCF FinTech Program (2019–2020); contributor to OpenStax open educational resources (2024).
- Sustained record of placing mentees into faculty positions, national laboratories, government, and industry.

TEACHING

Representative graduate teaching over the past decade; figures show enrollment and mean end-of-term student evaluation (5-point scale). Graduate courses except where marked.

Course	Term	Enr.	Eval.
CAP 6619 – Advanced Topics in ML	Spring 2024	32	4.84
CS 6463 – Special Topics: Trust in AI	Spring 2023	18	4.90
CS 6463 – Special Topics: Trust in AI	Spring 2022	8	5.00
CS 5633 – Analysis of Algorithms	Spring 2021	22	COVID-19
COT 5405 – Design & Analysis of Algorithms	Spring 2020	50	COVID-19
COT 5405 – Design & Analysis of Algorithms	Fall 2018	44	4.12
COT 5405 – Design & Analysis of Algorithms	Fall 2018	59	4.07

Course	Term	Enr.	Eval.
COT 5405 – Design & Analysis of Algorithms	Spring 2017	62	4.28
COT 5405 – Design & Analysis of Algorithms	Fall 2016	45	4.17
COT 5405 – Design & Analysis of Algorithms	Fall 2015	57	4.32
COT 5405 – Design & Analysis of Algorithms	Fall 2014	43	4.00
COT 5405 – Design & Analysis of Algorithms	Fall 2013	28	4.33

Evaluations on a 5-point scale; not collected in Spring 2020 and Spring 2021 (COVID-19). CAP 6619 reflects the instructor-interaction item.

POSTDOCTORAL RESEARCHERS

Partha Upadhyay (2025; Lecturer, UNC Greensboro) • Priyanka Kumar (2023; Asst. Prof., UT Permian Basin) • Lipismita Panigrahi (2023; Asst. Prof., SRM University-AP, India) • Sumit Tetarave (2022; Asst. Prof., KIIT, India) • Steven Fernandes (2020; Assoc. Prof., Creighton University).

GRADUATED PH.D. STUDENTS

Jodh Singh Pannu (2024; co-chair†; Research Associate/Scientist, UTSA) • Suraj Singireddy (2023; co-chair†; Senior ML Scientist, PayPal) • Mesut Ozdag (2020; Asst. Prof., UCF) • Sunny Raj (2020; Asst. Prof., Oakland University) • James Pyrich (2019; CEO) • Arfeen Khalid (2019; Senior ML Researcher, Comcast) • Dwaipayan Chakraborty (2019; Oak Ridge National Laboratory, Asst. Prof. Rowan University, and Google) • Amad Ul Hassen (2019; SUPARCO, Pakistan) • Alvaro Velasquez (2018; Air Force Research Laboratory and Asst. Prof., CU Boulder) • Emily Sassano (2018; Sanofi Pasteur) • Faraz Hussain (2016; Assoc. Prof., Clarkson University; G. Leavens co-advisor).

†Co-chaired at UTSA; Sushil Prasad served as the administrative graduating advisor of record following Jha's move from UTSA.

GRADUATED M.S. THESIS STUDENTS

Sourav Das (2023; Enterprise Information Governance Advisor, PenFed) • Junshuai Feng (2019; Senior Data Scientist, Hertz) • Yuan Shao (2019; Data Analyst, Hannover Re) • Anagha Sivakumar (2018; Software Engineer, CLX Engineering) • Andy Michel (2017; Qualcomm) • Arya Pourtabatabaie (2016; Cryptographer, Consensys).

PH.D. DISSERTATION COMMITTEE SERVICE

Served on 13 Ph.D. dissertation committees (2012–2023): Falonne Colbie (UTSA, 2023) • Kavita Kumari (UTSA, 2023) • Sahar Hooshmand (UCF, 2020) • John Singleton (UCF, 2018) • Yuyan Bao (UCF, 2018) • Rizwan Ashraf (UCF, 2015) • Soumyabrata Dey (UCF, 2014) • Aditya Reddy Kolli (UCF, 2014) • Amir R. Zamir (UCF, 2014) • Saptarshi Debroy (UCF, 2014) • Berkan Solmaz (UCF, 2013) • Mohammad Zubair Ahmad (UCF, 2012) • Yuan Li (UCF, 2012).

UNDERGRADUATE RESEARCH MENTORING

Mentored 25 undergraduate researchers (2011–2026), including NSF REU and Office of Undergraduate Research (OUR) awardees. **University of Florida:** Taran Raj (2026) • Hugh Tian (2026) • Yechan Kim (2026). **FIU:** Stephanie Painchault (2024–2025) • Jonathan Mathurin (2024) • Dorreen Vahidizar (2024) • Samuel Del Toro (2024–2025) • Andres Fernandez (2024–2025) • David Uloa (2025) • Gabriel Hubner Ferreira Lucchesi (2023–2025). **UCF:** Bernardin Dezius (NSF REU, 2017–2019) • Marcelino Galarza (NSF REU, 2017–2019) • Serra Abak (NSF REU, 2018–2019) • Dena Alawi (NSF REU, 2017–2018) • Angel Nunez (2016) • Howell Remington (URE energy award, 2015–2016) • Ryan Gonyon (OUR Award, 2015–2016) • Zubir Husein (2015–2016) • Nauman Javed (now MD/PhD, Harvard Medical School; Summer 2015) • Vincenzo Marconi (2014–2015) • Alvaro Velasquez (UCF Outstanding Thesis Award; 2013–2014) • Elias Davis (2013–2014) • Michael Poplavski (2012–2013) • Jordan Dubique (2012–2013) • Daniel Vivas-Garcia (2011–2013).

MENTEE HONORS

- Alvaro Velasquez: NSF Graduate Research Fellowship (2015); UCF "30 under 30" (2019); UCF Outstanding Thesis Award (2014).
- Emily Rebecca Sassano: NSF Graduate Research Fellowship (2012).
- Sven Thijssen: UCF ORC Fellowship (2020).
- Taran Raj: Emerging Scholars Program, University of Florida (2026).

CROSS-SECTOR COLLABORATION & INVITED ENGAGEMENT

- **National laboratories:** Argonne (DOE MEDAL), Oak Ridge (DOE/NNSA). **Industry:** General Motors, MathWorks, Royal Bank of Canada, Microsoft Research. **Agencies:** NSF, DARPA, DOE, AFRL/AFOSR, ONR, NGA, NNSA/ORNL, CyberFlorida. **Academic:** U.S. Military Academy at West Point.

INVITED MEETINGS, PANELS & TALKS

- **2026:** Panelist, SciFM 26, the 3rd Conference on Foundational Models and AI Agents for Science, University of Chicago (May 2026); competitively selected talk, *Intrinsic AI Assurance: Metacognition and Formally Verified Reasoning in Foundation Model Agents*, 26th High Confidence Software and Systems (HCSS) Conference, Annapolis, MD.
- **2025:** Competitively selected talk, *Functors as Bridges between AI-Generated Code and Formal Models for High-Confidence Software Systems*, 25th High Confidence Software and Systems (HCSS) Conference, Annapolis, MD, a U.S. Government, national-laboratory, and academic venue convened under the NITRD and NSA Science of Security programs.
- **2024:** DOE Workshops on Analog Computing and Neuromorphic Computing; DARPA PI Meetings (April, September); DoE PI Meeting (February); ONR Science of AI PI Meeting (May); NSF Workshop on Autonomous & Unmanned Systems (Baltimore; attended virtually); Mini-Symposium on Trustworthiness & Privacy in Distributed Learning, SIAM Conference on Mathematics of Data Science (MDS24).
- **2023:** Invited Speaker, Quantum Algorithm Design Automation (QADA), co-located with IEEE QCE 2023.
- **2022:** DoE ASCR Workshop on Visualization (January); DARPA GARD PI Meeting (April); ONR Science of AI PI Meeting (April).
- **2021:** DARPA GARD PI Meeting (September); DOE NNSA Workshop on Next-Generation AI for Proliferation Detection: Domain-Aware Methods (February); ONR Science of AI PI Meeting (April).
- **2020:** DARPA GARD PI Meeting (September); ONR Science of AI PI Meeting (April).
- **2016:** Invited Speaker, SRC Workshop on EDA/BDA Interaction Roadmap, Newcastle University, England.
- **2014:** Invited Talk, Numerical Software Verification Workshop, Vienna Summer of Logic, Austria.
- **2013:** Invited Talks at the SIAM Southeastern Atlantic Section meeting (Oak Ridge National Laboratory / University of Tennessee) and the CS Colloquium, University of Colorado Boulder.
- **2012:** Invited Talk, 20th High Performance Computing Symposium (HPC).
- **2010:** Invited Talk, BioPathways SIG, Intelligent Systems for Molecular Biology (ISMB).

PATENTS & TECHNOLOGY TRANSFER

- *System & Method for Path-Based In-Memory Computing.* US App. 2024/0311038 A1 (2024; application pending). UCF Research Foundation & UT System. record

- *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. record
- *3-D Crossbar Architecture for In-Memory Computing of Graph Transitive Closure.* US 11,538,989 B2 (2022). UCF Research Foundation. record
- *Stochastic Computational Model Parameter Synthesis System.* US 9,558,300 B2 (2017). CMU & UCF Research Foundation.
- *Computation of Boolean Formulas using Sneak Paths in Crossbar Computing.* US 9,319,047 B2 (2016). UCF Research Foundation / U.S. Air Force. record
- *Object Relational Map Verification System.* US 7,702,695 B2 (2010). Microsoft Corporation. record

PROFESSIONAL MEMBERSHIPS

Senior Member, IEEE • Full Member, Sigma Xi.

COMPLETE PUBLICATION LIST

Curated for Sumit Kumar Jha (ORCID 0000-0003-0354-2940; DBLP 05/5046-1). Entries are numbered in career order, with the earliest work as no. 1 and the most recent as no. 170, listed most-recent first. Persistent identifiers (DOI, arXiv) are available via the linked records in the Selected Publications above and on the author's website.

2026

170. P. Nwaorgu, S. Singireddy, A. Beckus, A. McKinney, M. Alinejad, C. Enyioha, **S.K. Jha**, A. Velasquez, G.K. Atia. *Automaton Distillation: Neuro-Symbolic Transfer Learning for Deep Reinforcement Learning*. TMLR, 2026.
169. 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 in Contextual Question Answering*. ACL (Findings), 2026.
168. V. Pramanik, M. Maliha, S. Jha, A. Velasquez, O. Kotevska, **S.K. Jha**. *Selective Amnesia using Contrastive Subnet Erasure for Class-Level Unlearning in Vision Models*. CVPR, 2026.
167. A. Babu, R. Kaur, N.D. Bastian, O. Kotevska, S. Jha, Y. Wu, **S.K. Jha**, A. Roy. *CTRL-STEER: Closed-Loop Neuron Activation Control in Vision-Language-Action Models*. CVPR Workshop on Visual Concepts (VisCon), 2026.
166. V. Pramanik, M. Maliha, N.D. Bastian, **S.K. Jha**. *Hessian-Enhanced Token Attribution (HETA): Interpreting Autoregressive Language Models*. ICLR, 2026.
165. V. Pramanik, M. Maliha, S. Jha, **S.K. Jha**. *Jailbreaking the Matrix: Nullspace Steering for Controlled Model Subversion*. ICLR, 2026.
164. H.H. Song, E. Bertino, A. Velasquez, H.H. Wang, Y. Shoshitaishvili, **S.K. Jha**. *AI for Cybersecurity: Research and Practice*. Wiley, 2026.

2025

163. W.H. English, D. Simon, **S.K. Jha**, R. Ewetz. *Grammar-Forced Translation of Natural Language to Temporal Logic using LLMs*. ICML, 2025.
162. C. Walker, **S.K. Jha**, R. Ewetz. *Metric-Driven Attributions for Vision Transformers*. ICLR, 2025.
161. C. Walker, M.R. Ahmed, **S.K. Jha**, R. Ewetz. *Explaining ViTs Using Information Flow*. AISTATS, 2025.
160. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, R. Ewetz. *LOGIC: Logic Synthesis for Digital In-Memory Computing*. ACM TODAES 30(2), 2025.
159. F. Rahat, M.S. Hossain, M.R. Ahmed, **S.K. Jha**, R. Ewetz. *Data Augmentation for Image Classification Using Generative AI*. WACV, 2025.
158. A. Roy, A. Cobb, R. Kaur, S. Jha, N. Bastian, A. Berenbeim, R. Thomson, I. Cruickshank, A. Velasquez, S. Jha. *Zero-Shot Detection of Out-of-Context Objects Using Foundation Models*. WACV, 2025.
157. D. Simon, S. Jha, R. Ewetz. *PATCHOUT: Adversarial Patch Detection and Localization using Semantic Consistency*. Neural Processing Letters 57(3), 2025.
156. N. Tirabassi, S.A.P. Kumar, S. Jha, A. Ramanathan. *MORAL: A Multimodal Reinforcement Learning Framework for Cognitive Intelligence in Autonomous Laboratories*. IEEE CogMI, 2025.
155. C.K. Jha, **S.K. Jha**, U. Schlichtmann, R. Drechsler. *Formal Verification Techniques and Reliability Methods for RRAM-based Computing-in-Memory* (Special Session). IEEE DFT, 2025.
154. R.S. Myana, **S.K. Jha**. *Explaining Protein Folding Networks Using Integrated Gradients and Attention Mechanisms*. ICCABS, 2025.
153. F. Rahat, M.S. Hossain, A. Ramanathan, S. Jha, H. Zheng, R. Ewetz. *Attr-RAG: Attribution-Guided Retrieval-Augmented Generation for Scientific Experiment Design*. ICMLA, 2025.

152. M.R. Ahmed, F. Rahat, M.S. Hossain, **S.K. Jha**, R. Ewetz. *Street2Air: A Framework for Synthesizing Aerial Vehicle Views from Ground Images*. ICMLA, 2025.
151. M.S. Hossain, **S.K. Jha**, H. Zheng, R. Ewetz. *Multitask Contrastive Learning using Task-Wise Training and Partitioned Embedding Space*. ICMLA, 2025.
150. A. Chavan, **S.K. Jha**, S. Raj. *Post-training Quantization without BN Statistics: A Data-Free Approach*. ICMLA, 2025.
149. D. Simon, C. Walker, S. Jha, R. Ewetz. *Detecting and Removing Adversarial Patches using Frequency Signatures*. IJCNN, 2025.
148. J.J. Modasiya, V.N. Kamineni, M.R.H. Rashed, M. Liehr, **S.K. Jha**, R. Ewetz. *On the Design and Fabrication of PATH-based In-Memory Computing Multipliers*. IEEE MDTS, 2025.
147. W.H. English, C. Walker, D. Simon, **S.K. Jha**, R. Ewetz. *Verifiable Natural Language to Linear Temporal Logic Translation: A Benchmark Dataset and Evaluation Suite*. arXiv, 2025.
146. P. Sinha, **S.K. Jha**, S. Raj. *Circuit Partitioning Using Large Language Models for Quantum Compilation and Simulations*. arXiv, 2025.
145. T. Rahman, S.A.P. Kumar, S. Jha, A. Ramanathan. *ACE-RLHF: Automated Code Evaluation and Socratic Feedback Generation Tool using Large Language Models and Reinforcement Learning with Human Feedback*. arXiv, 2025.
144. S. Kumar, S. Damodaran, N.K. Kuruba, S. Jha, A. Ramanathan. *DML-RAM: Deep Multimodal Learning Framework for Robotic Arm Manipulation using Pre-trained Models*. arXiv, 2025.
143. S.G.S. Pula, S.A.P. Kumar, S. Jha, A. Ramanathan. *Enhanced Penalty-based Bidirectional Reinforcement Learning Algorithms*. arXiv, 2025.
142. V. Pramanik, S. Jha, A. Velasquez, **S.K. Jha**. *Fact or Hallucination? An Entropy-based Framework for Attention-wise Usable Information in LLMs*. preprint, 2025.

2024

141. I. Alkhouri, **S.K. Jha**, A. Beckus, G.K. Atia, S. Jha, R. Ewetz, A. Velasquez. *Exploring the Predictive Capabilities of AlphaFold Using Adversarial Protein Sequences*. IEEE TAI, 2024.
140. C. Walker, **S.K. Jha**, K. Chen, R. Ewetz. *Integrated Decision Gradients: Compute Your Attributions Where the Model Makes Its Decision*. AAAI, 2024.
139. **S.K. Jha**, S. Jha, R. Ewetz, A. Velasquez. *On the Design of Novel Attention Mechanism for Enhanced Efficiency of Transformers*. DAC, 2024.
138. K. Kumari, M. Jadliwala, **S.K. Jha**, A. Maiti. *Towards a Game-Theoretic Understanding of Explanation-Based Membership Inference Attacks*. GameSec, 2024.
137. S. Thijssen, M.R.H. Rashed, M.R. Ahmed, S. Singireddy, **S.K. Jha**, R. Ewetz. *Equivalence Checking for Flow-Based Computing using Iterative SAT Solving*. ICCAD, 2024.
136. S. Thijssen, M.R.H. Rashed, S. Jha, R. Ewetz. *Synthesis of Compact Flow-based Computing Circuits from Boolean Expressions*. DAC, 2024.
135. M.R.H. Rashed, S. Thijssen, D. Simon, S. Jha, R. Ewetz. *Execution Sequence Optimization for Processing In-Memory using Parallel Data Preparation*. DAC, 2024.
134. S. Thijssen, M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *READ-based In-Memory Computing using Sentential Decision Diagrams*. ASP-DAC, 2024.
133. S. Thijssen, M.R.H. Rashed, H. Zheng, **S.K. Jha**, R. Ewetz. *Towards Area-Efficient Path-Based In-Memory Computing using Graph Isomorphisms*. ASP-DAC, 2024.
132. **S.K. Jha**, S. Jha, R. Ewetz, A. Velasquez. *Co-synthesis of Code and Formal Models using Large Language Models and Functors*. MILCOM, 2024.
131. **S.K. Jha**, S. Jha, M.R.H. Rashed, R. Ewetz, A. Velasquez. *Automated Synthesis of Hardware Designs using Symbolic Feedback and Grammar-Constrained Decoding in LLMs*. NAECON, 2024.
130. **S.K. Jha**, S. Jha, R. Ewetz, A. Velasquez. *Solving Mystery Planning Problems using Category Theory,*

Functors, and Large Language Models. ICAA, 2024.

129. W. English, D. Simon, R. Ahmed, S. Jha, R. Ewetz. *Neuro-Symbolic Program Synthesis for Multi-Hop Natural Language Navigation*. ICAA, 2024.
128. W. English, D. Simon, **S.K. Jha**, R. Ewetz. *NSP: A Neuro-Symbolic Natural Language Navigational Planner*. ICMLA, 2024.
127. S. Jha, **S.K. Jha**, A. Velasquez. *Neuro-Symbolic Generative AI Assistant for System Design*. ACM/IEEE MEMOCODE, 2024.
126. J. Brogan, O. Kotevska, A. Torres, S. Jha, M. Adams. *Improving Robustness of Spectrogram Classifiers with Neural Stochastic Differential Equations*. IEEE MLSP, 2024.
125. L.L. Pullum, **S.K. Jha**, R. Ewetz. *Intelligence, Surveillance and Reconnaissance Task Specifications in Temporal Logics*. MILCOM, 2024.
124. V. Pramanik, M. Maliha, **S.K. Jha**. *Human Fatality Estimation in Aircraft Accidents*. NAECON, 2024.
123. M.S. Hossain, **S.K. Jha**, C. Walker, R. Ewetz. *Out-of-Distribution Detection for Contrastive Models Using Angular Distance Measures*. ICMLA, 2024.
122. E. Bethany, M. Bethany, J.A.N. Flores, **S.K. Jha**, P. Najafirad. *Jailbreaking Large Language Models with Symbolic Mathematics*. arXiv, 2024.
121. A. Nunez, N.T. Islam, **S.K. Jha**, P. Najafirad. *AutoSafeCoder: A Multi-Agent Framework for Securing LLM Code Generation through Static Analysis and Fuzz Testing*. arXiv, 2024.

2023

120. S. Jha, **S.K. Jha**, P. Lincoln, N.D. Bastian, A. Velasquez, S. Neema. *Dehallucinating Large Language Models Using Formal Methods Guided Iterative Prompting*. IEEE ICAA, 2023.
119. **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.
118. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, F. Yao, R. Ewetz. *STREAM: Toward READ-based In-Memory Computing for Streaming-based Processing*. IEEE TCAD, 2023.
117. S. Thijssen, M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *PATH: Evaluation of Boolean Logic using Path-Based In-Memory Computing Systems*. IEEE TCAD, 2023.
116. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, R. Ewetz. *Automated Synthesis for In-Memory Computing*. ICCAD, 2023.
115. M.R.H. Rashed, S. Thijssen, **S.K. Jha**, H. Zheng, R. Ewetz. *Path-Based Processing using In-Memory Systolic Arrays for Accelerating Data-Intensive Applications*. ICCAD, 2023.
114. S. Thijssen, S. Singireddy, M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *Verification of Flow-Based Computing Systems using Bounded Model Checking*. ICCAD, 2023.
113. S. Thijssen, M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *UpTime: Towards Flow-Based In-Memory Computing with High Fault-Tolerance*. DAC, 2023.
112. S. Singireddy, M.R.H. Rashed, S. Thijssen, R. Ewetz, **S.K. Jha**. *Input-Aware Flow-Based In-Memory Computing*. ICCD, 2023.
111. M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *Discovering the In-Memory Kernels of 3D Dot-Product Engines*. ASP-DAC, 2023.
110. S. Thijssen, **S.K. Jha**, R. Ewetz. *FLOW-3D: Flow-Based Computing on 3D Nanoscale Crossbars with Minimal Semiperimeter*. ASP-DAC, 2023.
109. C. Walker, D. Simon, **S.K. Jha**, R. Ewetz. *Adversarial Pixel and Patch Detection using Attribution Analysis*. MILCOM, 2023.
108. **S.K. Jha**, S. Jha, R. Ewetz, A. Velasquez. *Neural Stochastic Differential Equations for Robust and Explainable Analysis of Electromagnetic Unintended Radiated Emissions*. MILCOM, 2023.
107. M.S. Hossain, M.R. Ahmed, L. Pullum, S. Jha, R. Ewetz. *Neuro-Symbolic Representations of 3D*

Scenes using Universal Scene Description Language. NeSy (NeurIPS Workshop), 2023.

106. I. Alkhouri, S. Jha, A. Beckus, G. Atia, A. Velasquez, R. Ewetz, A. Ramanathan, S. Jha. *On the Robustness of AlphaFold: A COVID-19 Case Study*. arXiv, 2023.

2022

105. N. Uysal, B. Zhang, **S.K. Jha**, R. Ewetz. *XMAP: Programming Memristor Crossbars for Analog Matrix-Vector Multiplication: Toward High Precision Using Representable Matrices*. IEEE TCAD, 2022.
104. **S.K. Jha**, R. Ewetz, A. Velasquez, A. Ramanathan, S. Jha. *Shaping Noise for Robust Attributions in Neural Stochastic Differential Equations*. AAAI, 2022.
103. **S.K. Jha**, A. Velasquez, R. Ewetz, L. Pullum, S. Jha. *ExplainIt!: A Tool for Computing Robust Attributions of DNNs*. IJCAI (Demonstrations), 2022.
102. M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *Logic Synthesis for Digital In-Memory Computing*. ICCAD, 2022.
101. S. Thijssen, **S.K. Jha**, R. Ewetz. *PATH: Evaluation of Boolean Logic using Path-based In-Memory Computing*. DAC, 2022.
100. S. Thijssen, **S.K. Jha**, R. Ewetz. *Equivalence Checking for Flow-Based Computing*. ICCD, 2022.
99. M.R.H. Rashed, A. Awad, **S.K. Jha**, R. Ewetz. *Towards Resilient Analog In-Memory Deep Learning via Data Layout Re-Organization*. DAC, 2022.
98. M.R.H. Rashed, **S.K. Jha**, F. Yao, R. Ewetz. *Hybrid Digital-Digital In-Memory Computing*. DATE, 2022.
97. A. Michel, **S.K. Jha**, R. Ewetz. *A Survey on the Vulnerability of Deep Neural Networks against Adversarial Attacks*. Progress in Artificial Intelligence 11(2), 2022.
96. **S.K. Jha**, R. Ewetz, A. Velasquez, S. Jha. *Responsible Reasoning with Large Language Models and the Impact of Proper Nouns*. NeurIPS Workshop (TSRML), 2022.
95. S. Singireddy, R. Ewetz, S. Jha. *Deep Learning Toolkit-Driven Equivalence Checking of Flow-Based Computing Systems*. IEEE AICAS, 2022.
94. S.L. Fernandes, S. Krivic, P. Sharma, **S.K. Jha**. *Attribution-Based Confidence Metric for Detection of Adversarial Attacks on Breast Histopathological Images*. ECCV Workshop, 2022.
93. K.A. Zubair, **S.K. Jha**, D. Mohaisen, C. Hughes, A. Awad. *FAT-PIM: Low-Cost Error Detection for Processing-In-Memory*. arXiv, 2022.
92. K. Kumari, M. Jadliwala, **S.K. Jha**, A. Maiti. *A Game-Theoretic Understanding of Repeated Explanations in ML Models*. arXiv, 2022.

2021

91. **S.K. Jha**, I.I. Mandoiu, S. Rajasekaran, P. Skums, A. Zelikovsky. *Special Issue: 10th International Computational Advances in Bio and Medical Sciences (ICCABS 2020)*. Journal of Computational Biology, 2021.
90. **S.K. Jha**, I.I. Mandoiu, S. Rajasekaran, P. Skums, A. Zelikovsky (eds.). *Computational Advances in Bio and Medical Sciences — 10th International Conference (ICCABS 2020), Revised Selected Papers*. Springer LNCS 12686, 2021.
89. S. Jha, R. Ewetz, A. Velasquez, S. Jha. *On Smoother Attributions using Neural Stochastic Differential Equations*. IJCAI, 2021.
88. M.R.H. Rashed, **S.K. Jha**, R. Ewetz. *Hybrid Analog-Digital In-Memory Computing*. ICCAD, 2021.
87. S. Channamadhavuni, S. Thijssen, **S.K. Jha**, R. Ewetz. *Accelerating AI Applications using Analog In-Memory Computing: Challenges and Opportunities*. GLSVLSI, 2021.
86. S. Thijssen, **S.K. Jha**, R. Ewetz. *COMPACT: Flow-Based Computing on Nanoscale Crossbars with Minimal Semiperimeter and Maximum Dimension*. IEEE TCAD, 2021.
85. S. Rafiq, J. Hazra, M. Liehr, K. Beckmann, M. Abedin, J.S. Pannu, **S.K. Jha**. *Investigation of*

ReRAM Variability on Flow-Based Edge Detection Computing Using HfO2-Based ReRAM Arrays. IEEE TCAS-I, 2021.

84. A. Velasquez, **S.K. Jha**, R. Ewetz, S. Jha. *Automated Synthesis of Quantum Circuits using Symbolic Abstractions and Decision Procedures*. ISCAS, 2021.
83. **S.K. Jha**, A. Ramanathan, R. Ewetz, A. Velasquez, S. Jha. *Protein Folding Neural Networks Are Not Robust*. arXiv, 2021.
82. A. Ramanathan, **S.K. Jha**. *Adversarial Attacks against AI-driven Experimental Peptide Design Workflows*. XLOOP Workshop, 2021.

2020

81. S. Fernandes, S. Raj, R. Ewetz, J.S. Pannu, **S.K. Jha**, E. Ortiz, I. Vintila, M. Salter. *Detecting Deepfake Videos using Attribution-Based Confidence Metric*. CVPR Workshop, 2020.
80. S.L. Fernandes, **S.K. Jha**. *Adversarial Attack on Deepfake Detection using RL based Texture Patches*. ECCV Workshop, 2020.
79. S. Raj, J.S. Pannu, S.L. Fernandes, A. Ramanathan, L.L. Pullum, **S.K. Jha**. *Attacking NIST Biometric Image Software using Nonlinear Optimization*. Pattern Recognition Letters 131, 2020.
78. N. Uysal, B. Zhang, **S.K. Jha**, R. Ewetz. *DP-MAP: Towards Resistive Dot-Product Engines with Improved Precision*. ICCAD, 2020.
77. J.S. Pannu, S. Raj, S.L. Fernandes, D. Chakraborty, S. Rafiq, N. Cady, **S.K. Jha**. *Design and Fabrication of Flow-Based Edge Detection Memristor Crossbar Circuits*. IEEE TCAS-II, 2020.
76. J.W. Bentley, D. Gibney, G. Hoppenworth, **S.K. Jha**. *Quantifying Membership Inference Vulnerability via Generalization Gap and Other Model Metrics*. arXiv, 2020.
75. **S.K. Jha**, S. Jha, R. Ewetz, S. Raj, A. Velasquez, L.L. Pullum, A. Swami. *An Extension of Fano's Inequality for Characterizing Model Susceptibility to Membership Inference Attacks*. arXiv, 2020.
74. D. Chakraborty, A. Michel, J.S. Pannu, S. Raj, S.C. Satapathy, S.L. Fernandes, **S.K. Jha**. *Automated Synthesis of Memristor Crossbars using Deep Neural Networks*. Intelligent Data Engineering and Analytics, 2020.

2019

73. M. Ozdag, S. Raj, S. Fernandes, A. Velasquez, L. Pullum, **S.K. Jha**. *On the Susceptibility of Deep Neural Networks to Natural Perturbations*. AISafety Workshop @ IJCAI, 2019.
72. S. Fernandes, S. Raj, E. Ortiz, I. Vintila, M. Salter, G. Urosevic, S. Jha. *Predicting Heart Rate Variations of Deepfake Videos using Neural ODE*. ICCV Workshop, 2019.
71. S. Jha, S. Raj, S. Fernandes, **S.K. Jha**, S. Jha, B. Jalaian, G. Verma, A. Swami. *Attribution-Based Confidence Metric for Deep Neural Networks*. NeurIPS, 2019.
70. D. Chakraborty, S. Raj, J.C. Gutierrez, T. Thomas, **S.K. Jha**. *Input-Aware Flow-Based Computing on Memristor Crossbars with Applications to Edge Detection*. IEEE JETCAS, 2019.
69. S. Fernandes, S. Raj, E. Ortiz, I. Vintila, **S.K. Jha**. *Directed Adversarial Attacks on Fingerprints using Attributions*. ICB, 2019.
68. S. Jha, S. Raj, S.L. Fernandes, **S.K. Jha**, S. Jha, G. Verma, B. Jalaian, A. Swami. *Attribution-Driven Causal Analysis for Detection of Adversarial Examples*. arXiv, 2019.
67. S. Raj, S.L. Fernandes, A. Michel, **S.K. Jha**. *Towards AI-driven Predictive Modeling of Gas Turbines using Big Data*. AIAA Propulsion and Energy Forum, 2019.
66. J.S. Pannu, S. Raj, S.L. Fernandes, **S.K. Jha**, D. Chakraborty, S. Rafiq, N. Cady. *Data-Driven Approximate Edge Detection using Flow-Based Computing on Memristor Crossbars*. IEEE Albany Nanotechnology Symposium, 2019.

2018

65. A. Velasquez, **S.K. Jha**. *3D Crosspoint Memory as a Parallel Architecture for Computing Network Reachability*. ICCD, 2018.
64. A.U. Hassen, D. Chakraborty, **S.K. Jha**. *Free Binary Decision Diagram-Based Synthesis of Compact Crossbars for In-Memory Computing*. IEEE TCAS-II, 2018.
63. S. Jha, S. Raj, **S.K. Jha**, N. Shankar. *Duality-Based Nested Controller Synthesis from STL Specifications for Stochastic Linear Systems*. FORMATS, 2018.
62. A. Velasquez, **S.K. Jha**. *In-Memory Computing using Paths-Based Logic and Heterogeneous Components*. DATE, 2018.
61. A. Velasquez, **S.K. Jha**. *Brief Announcement: Parallel Transitive Closure within 3D Crosspoint Memory*. SPAA, 2018.
60. A.U. Hassen, S.A. Khokhar, H.A. Butt, **S.K. Jha**. *Free BDD Based CAD of Compact Memristor Crossbars for In-Memory Computing*. NANOARCH, 2018.
59. A. Khalid, **S.K. Jha**. *Calibration of Rule-Based Stochastic Biochemical Models using Statistical Model Checking*. IEEE BIBM, 2018.
58. A. Khalid, **S.K. Jha**. *Parameter Estimation of Stochastic Biochemical Models using Multiple Hypothesis Testing*. IEEE ICCABS, 2018.
57. S. Raj, **S.K. Jha**. *Predicting Success in Undergraduate Parallel Programming via Probabilistic Causality Analysis*. IEEE IPDPS Workshop, 2018.
56. L. Pullum, C. Steed, **S.K. Jha**, A. Ramanathan. *Mathematically Rigorous Verification and Validation of Scientific Machine Learning*. ORNL Technical Report, 2018.

2017

55. S. Raj, F. Hussain, Z. Husein, N. Torosdagli, D. Turgut, N. Deo, S. Pattanaik, C.C. Chang, **S.K. Jha**. *A Theorem Proving Approach for Automatically Synthesizing Visualizations of Flow Cytometry Data*. BMC Bioinformatics, 2017.
54. S. Raj, L. Pullum, A. Ramanathan, **S.K. Jha**. *SATYA: Defending Against Adversarial Attacks Using Statistical Hypothesis Testing*. FPS, 2017.
53. **S.K. Jha**, A. Khalid. *Calibration of Stochastic Biochemical Models against Behavioral Temporal Logic Specifications*. IEEE ICCABS, 2017.
52. D. Chakraborty, **S.K. Jha**. *Automated Synthesis of Compact Crossbars for Sneak-Path Based In-Memory Computing*. DATE, 2017.
51. D. Chakraborty, **S.K. Jha**. *Design of Compact Memristive In-Memory Computing Systems using Model Counting*. ISCAS, 2017.
50. D. Chakraborty, S. Raj, J.C. Gutierrez, T. Thomas, **S.K. Jha**. *In-Memory Execution of Compute Kernels using Flow-Based Memristive Crossbar Computing*. IEEE ICRC, 2017.
49. S. Raj, D. Chakraborty, **S.K. Jha**. *In-Memory Flow-Based Stochastic Computing on Memristor Crossbars using Bit-Vector Stochastic Streams*. IEEE-NANO, 2017.
48. D. Chakraborty, S. Raj, **S.K. Jha**. *A Compact 8-bit Adder Design using In-Memory Memristive Computing: Towards Solving the Feynman Grand Prize Challenge*. NANOARCH, 2017.
47. A. Ramanathan, L. Pullum, Z. Husein, S. Raj, N. Torosdagli, S. Pattanaik. *Adversarial Attacks on Computer Vision Algorithms using Natural Perturbations*. IC3, 2017.
46. S. Raj, **S.K. Jha**, A. Ramanathan, L.L. Pullum. *Work-in-Progress: Testing Autonomous Cyber-Physical Systems using Fuzzing Features from Convolutional Neural Networks*. EMSOFT, 2017.
45. A. Velasquez, **S.K. Jha**. *Computation of Boolean Matrix Chain Products in 3D ReRAM*. ISCAS, 2017.
44. S. Raj, **S.K. Jha**, L.L. Pullum, A. Ramanathan. *Statistical Hypothesis Testing using CNN Features for Synthesis of Adversarial Counterexamples to Human and Object Detection Vision Systems*. ORNL Technical Report, 2017.

2016

43. A. Ramanathan, L.L. Pullum, F. Hussain, D. Chakraborty, **S.K. Jha**. *Integrating Symbolic and Statistical Methods for Testing Intelligent Systems: Applications to Machine Learning and Computer Vision*. DATE, 2016.
42. Z. Alamgir, K. Beckmann, N. Cady, A. Velasquez, **S.K. Jha**. *Flow-Based Computing on Nanoscale Crossbars: Design and Implementation of Full Adders*. ISCAS, 2016.
41. A. Velasquez, **S.K. Jha**. *Parallel Boolean Matrix Multiplication in Linear Time using Rectifying Memristors*. ISCAS, 2016.
40. A.U. Hassen, B. Chandrasekar, **S.K. Jha**. *Automated Synthesis of Stochastic Computational Elements using Decision Procedures*. ISCAS, 2016.
39. A. Velasquez, P. Wojciechowski, K. Subramani, S.L. Drager, **S.K. Jha**. *The Cardinality-Constrained Paths Problem: Multicast Data Routing in Heterogeneous Communication Networks*. IEEE NCA, 2016.

2015

38. A. Velasquez, **S.K. Jha**. *Automated Synthesis of Crossbars for Nanoscale Computing using Formal Methods*. NANOARCH, 2015.
37. A. Velasquez, **S.K. Jha**. *Fault-Tolerant In-Memory Crossbar Computing using Quantified Constraint Solving*. ICCD, 2015.
36. F. Hussain, C.J. Langmead, Q. Mi, J. Dutta-Moscato, Y. Vodovotz, **S.K. Jha**. *Automated Parameter Estimation for Biological Models using Bayesian Statistical Model Checking*. BMC Bioinformatics 16, 2015.
35. R. Saha, J. Esparza, **S.K. Jha**, M. Mukund, P.S. Thiagarajan. *Distributed Markov Chains*. VMCAI, 2015.
34. F. Hussain, Z. Husein, N. Torosdagli, N. Deo, S. Pattanaik, C.C. Chang. *SANJAY: Automatically Synthesizing Visualizations of Flow Cytometry Data using Decision Procedures*. IEEE ICCABS, 2015.

2014

33. F. Hussain, **S.K. Jha**, S. Jha, C.J. Langmead. *Parameter Discovery in Stochastic Biological Models using Simulated Annealing and Statistical Model Checking*. Int. J. Bioinformatics Research and Applications, 2014.
32. F. Hussain, A. Velasquez, E. Sassano, **S.K. Jha**. *Putting Humpty-Dumpty Together: Mining Causal Mechanistic Biochemical Models from Big Data*. IEEE ICCABS, 2014.
31. A. Velasquez, **S.K. Jha**. *Parallel Computing using Memristive Crossbar Networks: Nullifying the Processor-Memory Bottleneck*. IDT, 2014.
30. F. Hussain, A. Ramanathan, L.L. Pullum, **S.K. Jha**. *EpiSpec: A Formal Specification Language for Parameterized Agent-Based Models against Epidemiological Ground Truth*. IEEE ICCABS, 2014.
29. F. Hussain, R.G. Dutta, **S.K. Jha**, C.J. Langmead, S. Jha. *Parameter Discovery for Stochastic Biological Models against Temporal Behavioral Specifications using an SPRT-based Metric for Simulated Annealing*. IEEE ICCABS, 2014.
28. F. Hussain, N. Deo, **S.K. Jha**. *Early Adoption: High-Performance Computing for Big Data; Introducing Parallel Programming and Big Data in the Core Algorithms Curriculum*. NSF/TCPP Workshop, 2014.
27. A.K. Ghosh, F. Hussain, S. Jha, C.J. Langmead, **S.K. Jha**. *Discovering Rare Behaviours in Stochastic Differential Equations using Decision Procedures*. Int. J. Bioinformatics Research and Applications 10(4-5), 2014.
26. **S.K. Jha**, S. Jha, M. Mukund, R. Saha, P.S. Thiagarajan. *Distributed Markov Chains*. arXiv, 2014.

2013

25. N. Deo, **S.K. Jha**, F. Hussain, M. Vasudevan. *Introducing Parallel Programming across the Undergraduate Curriculum through an Interdisciplinary Course on Computational Modeling*. NSF/TCPP

Workshop, 2013.

24. A. Petkova, **S.K. Jha**, N. Deo. *Discriminative Stochastic Models for Complex Networks Derived from Flow Cytometry Big Data*. SE Int. Conf. Combinatorics, Graph Theory, 2013.

2012

23. A.R. Kolli, F. Sommerhage, P. Molnar, J.E. Hood, J.J. Jenkins, F. Hussain, A.K. Ghosh, **S.K. Jha**, J.J. Hickman. *A Computational Metabolic Model of the NG108-15 Cell for High Content Drug Screening with Electrophysiological Readout*. ACM BCB, 2012.
22. **S.K. Jha**, R.G. Dutta, C.J. Langmead, S. Jha, E. Sassano. *Synthesis of Insulin Pump Controllers from Safety Specifications using Bayesian Model Validation*. Int. J. Bioinformatics Research and Applications 8(3-4), 2012.
21. **S.K. Jha**, A. Ramanathan. *Quantifying Uncertainty in Epidemiological Models*. ASE/IEEE BioMedCom, 2012.
20. F. Hussain, R.G. Dutta, **S.K. Jha**, C.J. Langmead, S. Jha. *Parameter Discovery for Stochastic Computational Models in Systems Biology using Bayesian Model Checking*. IEEE ICCABS, 2012.
19. A.K. Ghosh, F. Hussain, **S.K. Jha**, C.J. Langmead, S. Jha. *Decision Procedure Based Discovery of Rare Behaviors in Stochastic Differential Equation Models of Biological Systems*. IEEE ICCABS, 2012.

2011

18. **S.K. Jha**, C.J. Langmead. *Synthesis and Infeasibility Analysis for Stochastic Models of Biochemical Systems using Statistical Model Checking and Abstraction Refinement*. Theoretical Computer Science 412(21), 2011.
17. **S.K. Jha**, C.J. Langmead. *Exploring Behaviors of SDE Models of Biological Systems using Change of Measures*. IEEE ICCABS, 2011.
16. **S.K. Jha**, C.J. Langmead, S. Mohalik, S. Ramesh. *When to Stop Verification? Statistical Trade-off between Expected Loss and Simulation Cost*. DATE, 2011.
15. **S.K. Jha**, G. Sukthankar. *Modeling and Verifying Intelligent Automotive Cyber-Physical Systems*. NIST/NSF/USCAR Workshop, 2011.

2010

14. **S.K. Jha**. *Model Validation and Discovery for Complex Stochastic Systems* (Ph.D. Thesis). Carnegie Mellon University, 2010.

2009

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.
12. C.J. Langmead, **S.K. Jha**. *Symbolic Approaches for Finding Control Strategies in Boolean Networks*. Journal of Bioinformatics and Computational Biology 7(2), 2009.

2008

11. S. Jha, **S.K. Jha**. *Randomization-Based Probabilistic Approach to Detect Trojan Circuits*. IEEE HASE, 2008.
10. E.M. Clarke, J.R. Faeder, C.J. Langmead, L.A. Harris, **S.K. Jha**, A. Legay. *Statistical Model Checking in BioLab: Applications to the Automated Analysis of T-Cell Receptor Signaling Pathway*. CMSB, 2008.
9. G. Frehse, **S.K. Jha**, B.H. Krogh. *A Counterexample-Guided Approach to Parameter Synthesis for Linear Hybrid Automata*. HSCC, 2008.
8. **S.K. Jha**. *d-IRA: A Distributed Reachability Algorithm for Analysis of Linear Hybrid Automata*. HSCC, 2008.
7. **S.K. Jha**, S. Jha. *Random Relaxation Abstractions for Bounded Reachability Analysis of Linear Hybrid*

Automata. IEEE HASE, 2008.

2007

6. **S.K. Jha**, B.H. Krogh, J.E. Weimer, E.M. Clarke. *Reachability for Linear Hybrid Automata using Iterative Relaxation Abstraction*. HSCC, 2007.
5. C.J. Langmead, **S.K. Jha**. *Predicting Protein Folding Kinetics via Temporal Logic Model Checking*. WABI, 2007.
4. K.K. Mehra, S.K. Rajamani, A.P. Sistla, **S.K. Jha**. *Verification of Object Relational Maps*. SEFM, 2007.

2006

3. S. Jiang, T.E. Fuhrman, **S.K. Jha**. *Model Checking for Fault Explanation*. IEEE CDC, 2006.

2005

2. E. Clarke, A. Fehnker, **S.K. Jha**, H. Veith. *Temporal Logic Model Checking* (book chapter). Handbook of Networked and Embedded Control Systems, 2005.
1. A. Fehnker, E. Clarke, **S.K. Jha**, B. Krogh. *Refining Abstractions of Hybrid Systems using Counterexample Fragments*. HSCC, 2005.