Tanmay Khandait

+1 (602) 632 3939 | tkhandai@asu.edu | linkedin.com | github.com | daittan.com

Education

Ph.D. in Computer Science Jan. 2023 - Dec. 2026
Arizona State University *GPA: 3.98/4.00*

MS in Computer Science Jan. 2021 - Dec. 2022
Arizona State University *GPA: 4.00/4.00*

Master's Thesis: Inside the Box: Analysing Cyber-physical Systems, Exploiting Models and Specifications

B.Tech. in Computer Science and Engineering Aug. 2015 - Jul. 2019
Indian Institute of Information Technology Vadodara *GPA: 7.52/10.00*

Bachelor's Thesis: Bi-Lateral Adaptive Switching System for Home Automation

Research Experience

Graduate Research Assistant Jun. 2021 – Present
Cyber-Physical Systems (CPS) Lab, Arizona State University *Tempe, AZ, USA*

- Conducting research on optimization-based verification and safe learning in Cyber-Physical Systems (CPS), with applications in autonomous systems and AI safety.
- Developed **HyperPart-X** and **Part-X**, stochastic algorithms providing probabilistic guarantees for system falsification and formal verification.
- Proposed a **multi-agent rollout framework for Bayesian Optimization**, outperforming TuRBO on benchmark problems; designed to serve as a scalable parallel layer for existing BO methods.
- Designed STL-based algorithms for generating **stealthy attacks** and falsifying temporal logic specifications in autonomous vehicle simulators and flight systems.
- Investigating **AI agent alignment and misalignment evaluation** through multi-objective optimization to develop metrics to identify adversarial or conflicting mission objectives.
- Worked on implementing **NNRepLayer**, a Mixed-Integer Quadratic Programming (MIQP) framework for repairing neural networks under safety constraints; achieved 5–10% improvement in constraint satisfaction for assistive robotic controllers.
- Built multi-fidelity optimization frameworks for parameter mining of temporal logic formulas and efficient hyperparameter tuning of large-scale neural networks.
- Optimized large-scale falsification and Bayesian optimization pipelines using distributed computing with **Ray** for scalable experimentation.
- Co-authored multiple publications in IEEE, ACM, and Springer venues; developed open-source research tools combining machine learning, optimization, and formal verification.

Research Associate Jul. 2019 – Nov. 2020
Production & Quantitative Methods Area, Indian Institute of Management Ahmedabad (IIM-A) *Ahmedabad, India*

- Designed a **gradient-based bilevel optimization framework** for hyperparameter tuning of neural networks, reducing search time by 3× compared to standard grid and random search.
- Led a project with the Indian Gold Policy Center (IGPC) to build a large-scale **financial news sentiment dataset** (11,400+ annotated samples) for commodity market analysis and forecasting.
- Developed deep learning–based **NLP models** (Word2Vec, ELMo, BERT) to predict market sentiment and price movements, achieving an F1 score above 93%.
- Contributed to statistical analysis establishing a significant correlation ($p < 0.05$) between news sentiment and gold price volatility; published results in peer-reviewed venues.

Engineering & Implementation Experience

Software Engineer / Research Engineer (Research Tools for CPS) Jun. 2021 – Present
Arizona State University – DARPA ARCOS, ASIMOV, and FIRE Programs *Tempe, AZ, USA*

- Engineered scalable distributed experimentation pipelines for probabilistic verification and Bayesian optimization algorithms (**Part-X**, **HyperPart-X**, **MARoBoSE**) using **Ray** clusters across four compute nodes; reducing runtime from 10+ hours to 2–3 hours.
- Designed and maintained **research-grade open-source libraries** (**Part-X**, **PySOAR**, **LSemiBO**, **CoNBO**) integrated with **S-TALIRO** for automated test generation and certification analysis of Cyber-Physical Systems.
- Contributed software, benchmarks, and verification results to DARPA's **ARCOS (Automated Rapid Certification of Software)** program, and developed evaluation and alignment tools for the **ASIMOV** and **FIRE** programs; presented outcomes at program QPRs and review meetings.

Summary of Selected Manuscripts

Pareto Adversarial Scenario Search (PASS), 2025 (Submitted)

- **Objective:** Develop a quantitative framework to evaluate alignment and misalignment between autonomous agents under multiple, potentially conflicting, mission and normative objectives.
- **Contribution:** Introduces the **PASS** method, a multi-objective adversarial scenario generation approach that discovers edge-case situations where AI agents perform sub-optimally or exhibit ethical conflicts, producing measurable alignment evidence for DARPA's ASIMOV program.

Conjunctive Bayesian Optimization (ConBO), 2025 (Submitted)

- **Objective:** Address the challenge of verifying systems against multiple conjunctive formal requirements efficiently.
- **Contribution:** Proposes **ConBO**, a novel Bayesian optimization framework that decomposes conjunctive verification problems into structured subspaces, enabling scalable falsification of Cyber-Physical Systems with guaranteed convergence.

HyperPart-X: Probabilistic Guarantees for Parameter Mining of Signal Temporal Logic, 2024 (Runtime Verification)

- **Objective:** Extend search-based test generation to parametric temporal logic specifications with formal probabilistic guarantees.
- **Contribution:** Presents **HyperPart-X**, an active parameter-mining algorithm that jointly explores input and specification parameter spaces to compute falsification level sets with finite-time confidence bounds, enabling scalable CPS verification.

Part-X: A Family of Stochastic Algorithms for Search-Based Test Generation, 2023 (IEEE T-ASE)

- **Objective:** Provide a probabilistically sound framework for automated test generation in Cyber-Physical Systems.
- **Contribution:** Introduces **Part-X**, a stochastic partitioning algorithm that offers finite-time probabilistic guarantees for falsification, forming the core of DARPA ARCOS's automated certification process.

Publications

2025

- **Khandait, T.**, & Pedrielli, G.(2025). **Pareto Adversarial Scenario Search (PASS): Generating Evidence for Autonomy Alignment Evaluation.** Submitted for review, July 2025.
- Chotaliya, S., **Khandait, T.**, & Pedrielli, G. (2025). **Conjunctive Bayesian Optimization (ConBO): A Scalable Approach to Cyber-Physical Systems Verification with Conjunctive Requirements.** Submitted for review, May 2025.
- Inman, J., **Khandait, T.**, Sankar, L., & Pedrielli, G. (2025). **POCAII: Parameter Optimization with Conscious Allocation using Iterative Intelligence.** Submitted for review, *INFORMS Journal on Computing (IJOC)*, February 2025. *arXiv preprint* arXiv:2505.11745.
- Abou-Mrad, C., **Khandait, T.**, Pedrielli, G., & Abbas, H. (2025). **Falsification and Control of CPS using the Language Set of Discrete-Time Temporal Logic.** In *Proceedings of the ACM/IEEE 16th International Conference on Cyber-Physical Systems (CPS-IoT Week 2025)*.

2024

- **Khandait, T.**, & Pedrielli, G. (2024). **HyperPart-X: Probabilistic Guarantees for Parameter Mining of Signal Temporal Logic Formulas in Cyber-Physical Systems.** In *Runtime Verification (RV 2024)*, Springer Nature. DOI
- **Khandait, T.**, Formica, F., Arcaini, P., Chotaliya, S., Fainekos, G., Hekal, A., Kundu, A., Lew, E., Loreti, M., Menghi, C., et al. (2024). **ARCH-COMP 2024 Category Report: Falsification.** In *International Workshop on Applied Verification for Continuous and Hybrid Systems (ARCH 2024)*, EasyChair.
- Sinha, A., **Khandait, T.**, & Mohanty, R. (2024). **A Gradient-Based Bilevel Optimization Approach for Tuning Regularization Hyperparameters.** *Optimization Letters, 18*(6), 1383–1404. DOI

2023

- Pedrielli, G., **Khandait, T.**, Cao, Y., Thibeault, Q., Huang, H., Castillo-Effen, M., & Fainekos, G. (2023). **Part-X: A Family of Stochastic Algorithms for Search-Based Test Generation with Probabilistic Guarantees.** *IEEE Transactions on Automation Science and Engineering, 21*(3), 4504–4525. DOI
- Majd, K., Clark, G., **Khandait, T.**, Zhou, S., Sankaranarayanan, S., Fainekos, G., & Amor, H. B. (2023). **Safe Robot Learning in Assistive Devices through Neural Network Repair.** *arXiv preprint* arXiv:2303.04431.
- Majd, K., Clark, G., **Khandait, T.**, Zhou, S., Sankaranarayanan, S., Fainekos, G., & Amor, H. B. (2023). **Certifiably-Correct Control Policies for Safe Learning and Adaptation in Assistive Robotics.** *arXiv preprint* arXiv:2303.06582.
- Thibeault, Q., **Khandait, T.**, Pedrielli, G., & Fainekos, G. (2023). **Search-Based Testing for Code Coverage and Falsification in Cyber-Physical Systems.** In *IEEE 19th International Conference on Automation Science and Engineering (CASE 2023)*. DOI

- Chandratre, A., Hernandez Acosta, T., **Khandait, T.**, Pedrielli, G., & Fainekos, G. (2023). **Stealthy Attacks Formalized as STL Formulas for Falsification of CPS Security.** In *ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2023)*. DOI
- **Khandait, T.**, Chandratre, A., Baptista, W., Pedrielli, G., & Fainekos, G. (2023). **Demo Abstract: Analysing CPS Security with Falsification on Microsoft Flight Simulator.** In *ACM HSCC 2023*. DOI
- Inman, J., **Khandait, T.**, Pedrielli, G., & Sankar, L. (2023). **Parameter Optimization with Conscious Allocation (POCA).** In *Winter Simulation Conference (WSC 2023)*. DOI
- Jiang, M. M., **Khandait, T.**, & Pedrielli, G. (2023). **CGPT: A Conditional Gaussian Process Tree for Grey-Box Bayesian Optimization.** In *Winter Simulation Conference (WSC 2023)*. DOI
- Menghi, C., Arcaini, P., Baptista, W., Ernst, G., Fainekos, G., Formica, F., Gon, S., **Khandait, T.**, Kundu, A., Pedrielli, G., et al. (2023). **ARCH-COMP 2023 Category Report: Falsification.** In *International Workshop on Applied Verification of Continuous and Hybrid Systems (ARCH 2023)*, EasyChair.

2022

- Ernst, G., Arcaini, P., Fainekos, G., Formica, F., Inoue, J., **Khandait, T.**, Mahboob, M. M., Menghi, C., Pedrielli, G., Waga, M., et al. (2022). **ARCH-COMP 2022 Category Report: Falsification with Unbounded Resources.** In *Applied Verification of Continuous and Hybrid Systems (ARCH 2022)*, EPiC Series in Computing, 90, 204–221. DOI

2021

- Sinha, A., **Khandait, T.** (2021). **Impact of News on the Commodity Market: Dataset and Results.** In *Future of Information and Communication Conference (FICC 2021)*, Springer. DOI
- Ernst, G., Arcaini, P., Bennani, I., Chandratre, A., Donzé, A., Fainekos, G., Frehse, G., Gaaloul, K., Inoue, J., **Khandait, T.**, et al. (2021). **ARCH-COMP 2021 Category Report: Falsification with Validation of Results.** In *ARCH@ADHS*, EPiC Series in Computing, 80, 133–152. DOI

Presentations & Talks

- **"ARCH-COMP Falsification Category Results."** Presented at *ADHS 2024 – IFAC Workshop on Analysis and Design of Hybrid Systems*, October 2024.
- **"MARoBoSE: Multi-Agent Rollout Bayesian Optimization for Scalable Experimentation."** Accepted for presentation at *INFORMS Annual Meeting 2025*, Atlanta, GA.

Reviewer Work

- IEEE Transactions on Automation Science and Engineering (IEEE T-ASE)
- ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS 2025)
- Science of Computer Programming (Elsevier)
- Journal of Simulation (Taylor & Francis)
- Flexible Services and Manufacturing Journal (Springer)
- ACM/IEEE International Conference on Embedded Software (EMSOFT 2025)
- IEEE International Conference on Automation Science and Engineering (CASE 2024)

Teaching

IEE 575: Applied Stochastic Operations Research Models Spring 2025, Spring 2024

Teaching Assistant, Arizona State University *Tempe, AZ, USA*

- Conducted lab sessions for graduate students, focusing on stochastic optimization, Monte Carlo simulation, and Bayesian optimization techniques.
- Assisted in developing Python-based instructional material and guiding student projects involving optimization and simulation models.
- Led hands-on sessions implementing Gaussian Process Regression and Bayesian optimization using Python's scientific libraries.

Technical Skills

- **Core Areas:** Optimization, Machine Learning, Reinforcement Learning, Formal Verification, Bayesian Optimization, Safe AI.
- **Programming:** Python, MATLAB, R, SQL.
- **Frameworks:** PyTorch, TensorFlow, Scikit-learn, Numpy, Pandas, OpenCV.
- **Tools:** Git, Docker, Android Studio, Flutter.