HOSSEIN HAJIPOUR

PRESENT ADDRESS
Im Sauerbrod 84
66123, Saarbruecken, Germany

CONTACT INFORMATION
Phone: +49 176 363 50091
E-mail: ho.hajipour@gmail.com
Website: hajipour.github.io

OBJECTIVE

Developing safe and adaptable AI agents capable of understanding and generating code to address real-world tasks across each stage of the software development life cycle.

RESEARCH INTEREST

AI for Code Generation and Code Understanding, Safe AI for Code, and Machine Learning.

PROFESSIONAL EXPERIENCE

- **CISPA Helmholtz Center for Information Security**, Ph.D. Researcher, Sep 2018 - Now.
  - Conducted research on AI code generation models, focusing on program repair, reverse engineering, and the analysis and enhancement of safety aspects in large language models for code.
  - Selected project: Developed HexaCoder, an innovative approach to improve LLMs' ability to generate secure code. HexaCoder reduced software vulnerability generation rates of LLMs by up to 85% while maintaining the output accuracy.
- **Max Planck Institute for Informatics**, Research Assistant, Jan 2018 - Aug 2018.
  - Developed a novel deep learning approach for monocular 3D shape reconstruction, achieving 36% higher accuracy than the baseline in reconstructing 3D models.
- **Max Planck Institute for Informatics**, Research Assistant, Apr 2017 - Dec 2017.
  - Designed and implemented a deep learning approach for automatic rendering artifacts correction.
- **Cluster of Excellence MMCI**, Back-end Developer, Oct 2015 - Mar 2017.
  - Implemented a bot to crawl and aggregate information on more than 1000 web pages.

EDUCATION

Saarland Univeristy, Saarbruecken, Germany Sep 2018 - Dec 2024 (Expected)
CISPA Helmholtz Center for Information Security
Ph.D. in Computer Science
Advisor : Prof. Dr. Mario Fritz

Saarland Univeristy, Saarbruecken, Germany Oct 2015 - Jul 2018
M.Sc. in Computer Science, **GPA**: 1.2 (94 out of 100)
Thesis: Weakly-supervised Surface Reconstruction Using Floating Radial Basis Functions.
Advisor : Prof. Dr. Christian Theobalt

Persian Gulf University, Bushehr, Iran Feb 2010 - Jun 2014
B.Sc. in Computer Engineering, **GPA**: 17.05 (85 out of 100)

PUBLICATION

1. **Hossein Hajipour**, Lea Schönherr, Thorsten Holz, Mario Fritz. "HexaCoder: Secure Code Generation via Oracle-Guided Synthetic Training Data". arXiv, Sep 2024, Link.
2. **Hossein Hajipour**, Ning Yu, Cristian-Alexandru Staicu, and Mario Fritz. "SimSCOOD: Systematic Analysis of Out-of-Distribution Generalization in Fine-tuned Source Code Models". NAACL Findings, Jun 2024, Link.
3. **Hossein Hajipour**, Keno Hassler, Thorsten Holz, Lea Schönherr, and Mario Fritz. "CodeLMSec Benchmark: Systematically Evaluating and Finding Security Vulnerabilities in Black-Box Code Language Models". IEEE SaTML, Apr 2024, Link.
4. **Hossein Hajipour**, Mateusz Malinowski, and Mario Fritz. "IReEn: Reverse-Engineering of Black-Box Functions via Iterative Neural Program Synthesis". ECML PKDD Workshops, Springer. Sep 2021, Link.
5. **Hossein Hajipour**, Apratim Bhattacharya, Cristian-Alexandru Staicu, and Mario Fritz. "SampleFix: Learning to Generate Functionally Diverse Fixes". ECML PKDD Workshops. Sep 2021, Link.
6. **Hossein Hajipour**, Hamed B.Khourmuji, and Habib Rostami. "ODMA: A Novel Swarm-Evolutionary Metaheuristic Optimizer Inspired by Open Source Development Model and Communities." Soft Computing, Springer. Feb 2016, Link.
7. **Hossein Hajipour**, Hamed B.Khourmuji, Habib Rostami, and Rozita J.Oskouei. "ODMA: A New Metahueristic Optimization Algorithm Based On Open Source Development Model." ISDA'12. Nov 2012, Link.

ACADEMIC EXPERIENCE

- Thesis co-supervision: The Security Implications of AI Software Engineer Agents, Tobias Lorig, B.Sc., 2024.
- Reviewing: ACL'23, S&P'23, EuroS&P'22, CCS'22, EMNLP'(22, 23).
- Teaching Assistant of "Machine Learning in Cyber Security." CISPA Helmholtz Center for Information Security. 2018, 2019, 2020.
- Instructor of "Introduction to Web Application" ICT Institute of Persian Gulf University. 2015.
- Teaching Assistant of "Algorithm Design." and "Data Structures and Algorithms." Persian Gulf University. 2014, 2013.

HONORS AND AWARDS

- Fully funded Ph.D. studentship from CISPA Helmholtz Center for Information Security, 2018.
- German-French Ph.D. Workshop on Secure Big Data scholarship, 2018.
- Master thesis scholarship from Saarland University. 2018.
- Awarded 2nd place as a team at Startup Weekend, Bushehr, Iran, 2015.

SKILLS

- **Programming**
  - Python, C, C++ , CUDA.
- **Tools/Frameworks**
  - PyTorch, HuggingFace Transformers, NumPy, LangGraph, SciPy, Git.
- **Theory**
  - Large Language Models, Deep Learning, Program Synthesis, Statistical Learning.
- **Languages**
  - English (Fluent), German (Basic), Farsi/Persian (Native).