Masoud Jamshidiyantehrani

masoud.jamshidiyantehrani@usi.ch | +41-76-2162421 | LinkedIn — Scholar — GitHub

EDUCATION

Università della Svizzera italiana — Lugano, Switzerland
PhD in Computer and Information Systems Security/Information Assurance — 2024 — Present
Project: Cybersecurity for AI-Augmented Systems
Program: Part of the Sec4AI4Sec initiative, funded by the EU Horizon Europe program

University of Shiraz — Shiraz, Iran
MS in Computer Science (Cyber Security) — 2020 — 2023
GPA: 19.08/20 (Ranked 1st out of 9)
Thesis: Software Security Analysis for Finding Vulnerabilities in Smart Contracts

University of Fasa — Fasa, Iran
BSc in Computer Engineering — 2016 — 2020
GPA: 17.5/20 (Ranked 1st out of 47)
Bachelor's Project: Establishing An Online Class Environment

INTERESTS

- Autonomous Vehicles
- Software Security
- Adversarial Machine Learning
- Deep Learning
- AV Perception Security
- AI for Security

PUBLICATIONS

- **MJ Tehrani**, M Gabriel, J Kim, P Tonella, "Dynamic Deception: When Pedestrians Team Up to Fool Autonomous Cars", (Arxiv)
- **MJ Tehrani**, J Kim, P Tonella, "PCLA: A Framework for Testing Autonomous Agents in the CARLA Simulator", (FSE'25)
- **MJ Tehrani, et.al**, "A Taxonomy of System-Level Attacks on Deep Learning Models in Autonomous Vehicles", (TOSEM)
- **MJ Tehrani**, "Enhancing Smart Contract Security: Assessing Vulnerability with Code Complexity Metrics", (Arxiv)
- **Goshtasbi.A, et.al**, "AI-infused dissipative tactile sensing", Submitted to the IEEE 7th International Conference on Soft Robotics, (RoboSoft)
- **MJ Tehrani**, Arjomand, P., "Finding The Potential Accepted Answer on Stack Overflow: A Text Mining Approach " Transaction on Machine Intelligence

RESEARCH EXPERIENCE

Dynamic Deception: When Pedestrians Team Up to Fool Autonomous Cars — Sep 2025 — Present

- Designed a novel system-level adversarial threat model in which coordinated pedestrians act as dynamic carriers of physical adversarial patches.
- Created a stealthy adversarial stop-sign pattern camouflaged as a red camellia flower to ensure physical plausibility and real-world deployability.
- Developed coordinated multi-agent pedestrian strategies to maximize temporal persistence of adversarial signals within the vehicle's camera field of view.
- Implemented and evaluated the attack pipeline in the CARLA simulator against a state-of-the-art end-to-end autonomous driving agent.
- Replication package available on Github

PCLA: A Framework for Testing Autonomous Agents in the CARLA Simulator — Nov 2024 — Present

- The main benchmark for testing autonomous agents in the CARLA simulator, available open source on GitHub.
- PCLA provides a clear method to deploy Autonomous Driving Agents (ADAs) onto a vehicle without relying on the Leaderboard codebase.
- Enables easy switching between ADAs without requiring changes to CARLA versions or programming environments.
- Allows you to have multiple vehicles with different autonomous agents (requires high graphical memory).
- Provides the next movement action computed by the chosen agent, which can then be used in any desired application.
- Is fully compatible with the latest version of CARLA and independent of the Leaderboard's specific CARLA version.
- Includes 36 different high-performing ADAs trained with 27 additional training seeds.

A Taxonomy of System-Level Attacks on Deep Learning Models in Autonomous Vehicles — Sep 2024

- The first comprehensive taxonomy of security vulnerabilities that affect autonomous vehicles with deep learning components.
- The taxonomy identifies critical vulnerabilities, highlights areas for future research, and is useful for finding attacks that caused system-level failures in simulations or the real world.
- A companion GitHub repository is available for data mining and exploring the taxonomy without reading the full paper GitHub.

Enhancing Smart Contract Security: Assessing Vulnerability with Code Complexity Metrics January 2022 — September 2023
- Analyzed 21 complexity metrics and used machine learning classification models and correlation techniques to verify the connectivity between complexity and vulnerabilities in Solidity smart contracts.
- Used statistical techniques to find the correlation and the discriminative power of each metric

AI-infused dissipative tactile sensing November 2023
- Machine learning and deep learning models were used to learn the data from soft robots.
- Implementation of regression models such as MLP, SVR, linear regression, and polynomial regression for learning and predicting continuous numbers.

Finding The Potential Accepted Answer on Stack Overflow: A Text Mining Approach July 2021
- Independent research that focused on merging machine learning and text mining.
- Utilized sentiment analysis and NLP on Stack Overflow to predict the accepted answer.

SUPERVISION EXPERIENCE

Research Mentor & Supervision
Università della Svizzera italiana
- Co-supervised the master's thesis of Marco Gabriel, in collaboration with Professor Paolo Tonella.
- Guided research on adversarial attacks on autonomous vehicles using the CARLA simulator.
- Provided mentorship in research design, experimentation, and evaluation.
- Supported the development of technical and academic skills throughout a one-year project.
- The work concluded with a successful thesis defense (10/10 grade) and has strong potential for publication in a top-tier conference.

TEACHING EXPERIENCE

Graduate Teaching Assistant September 2024 — Present
Università della Svizzera italiana
Course name: Software Atelier 4 (2 times
Course name: Founders 2
Course name: Introduction to Fintech (2 times)

Graduate Teaching Assistant October 2021 — October 2022
University of Shiraz
Course name: Cryptological Mathematics

Undergraduate Teaching Assistant September 2019 — December 2019
University of Fasa
Course name: Data Structures
Course name: Fundamentals of Computer & Programming

COURSE PROJECTS

Bachelors' Project October 2019 — June 2020
Project: Establishing an online class environment
- Prepared servers of the University of Fasa for the online class platform
- Installed and maintained Moodle learning platform
- Delivered a high-quality and light-weight learning platform for online classes and online exams
- Instructed professors and students to use the platform

Cryptological Mathematics November 2020 — February 2021
Project: Simple Encryption and Decryption and its Cryptanalysis (Link)
- Implemented a simple encryption and decryption model using XOR operation and a binary key.

- Cryptanalyzed the algorithm using plain-text and cipher-text

Project: Affine Hill Cipher and its Cryptanalysis (Link)
- Implemented the affine hill cipher algorithm
- Cryptanalyzed the algorithm using plain-text and cipher-text

Project: CRT Factorization (Link)
- Programmed the Chinese remainder theorem for factorization

Project: Rabin Encryption (Link)
- Programmed the Rabin encryption system

Network Security November 2020 — February 2021

Project: Vigenère Cipher and its Cryptanalysis (Link)
- Implemented Vigenère cipher algorithm to encrypt and decrypt any file.
- Cryptanalyzed the algorithm using plain-text, cipher-text, and key's length
- Cryptanalyzed the algorithm using cipher-text and key's length
- Cryptanalyzed the algorithm using only the cipher-text

Project: DES (Link)
- Implemented the Data Encryption Standard.

Project: Wireshark
- Located, captured, and analyzed packages from Whatsapp and Telegram

Machine Learning March 2021 — June 2021

Project: Tic Tac Toe With AI (Link)
- Implemented Tic Tac Toe with AI using the "Function Approximation" algorithm.
- Extracted 11 features and passed to AI to learn.
- Systematized the program to be fully customizable. Every feature's weight can be seen and turned off or on. Learning rate, train iterations, and scores for winning, losing, and scoring a draw are adjustable. Can also choose who starts first, AI or human.

Project: Several ML Algorithms
- Implemented these algorithms from scratch: Decision Tree Classification and Regression, Adaboost and Bagging for normal and noisy data, K-means Clustering, Kernel KNN, Kernel Supervised PCA, and Ensemble Learning for Spectral Clustering from a 2020 paper

Database Security March 2021 — June 2021

Project: Data Encryption and Access Control (Link)
- Encrypted and Decrypted the columns and tables in SQL using Triple DES algorithm.
- Managed access control in the database using Virtual Private Databases (VPD)

Project: Database Security Management with Apache Cassandra
- Managed authentication and authorization as well as roles and permissions

Text Mining November 2020 — February 2021

Project: Words Similarity (Link)
- Executed text preprocessing using KNIME analytics platform.
- Utilized Wordnet to find hypernyms, hyponyms, and synonyms of each word.
- Calculated semantic distance and similarity between two words

Project: Text Mining Classification (Link)
- Classified texts from Wikipedia using only KNIME analytics platform

Project: Sentiment Analysis (Link)
- Analyzed the sentiments of Stack Overflow posts to find the accepted answer using several methods as well as Senti4SD and sentiment lexicons.

CERTIFICATES

ACM International Conference on the Foundations of Software Engineering (FSE) 2025 June 2025
Trondheim, Norway

7th Advanced Course on Data Science & Machine Learning June 2024
Tuscany, Italy

4th International Software Engineering Summer School (SIESTA 2024) September 2024
Bari, Italy

WORK EXPERIENCE

Full-Stack Web Developer 2017 — 2020
Farazgaman inc, Shiraz

- Project manager and lead developer
- Web development lecturer for junior employees
- WordPress plug-in developer
- Certificate of training under the subject of "Web Design and E-commerce Workshop" by IQS Academy (Certification Number: 38118467)

SKILLS

Languages: English (C2), Persian (Native), German (A1), Italian (A1)

Programming Languages: Python, C#, Java, C++, JavaScript

Softwares: CARLA Simulator, Linux and Git Terminals, GitLab, VS and VS Code, Wireshark, WordPress, LaTeX

REFERENCES

Prof. Dr. Paolo Tonella
Supervisor
Faculty of Informatics
Università della Svizzera italiana
paolo.tonella@usi.ch
Scholar

Dr. Jinhan Kim
Co-Supervisor
Faculty of Informatics
Università della Svizzera italiana
jinhan.kim@usi.ch
Scholar