Zahra Moti

PhD Candidate
Radboud University
The Netherlands

zahra.moti@ru.nl
zahramoti.com
zahra-moti
zahra7394

PhD candidate applying ML and LLMs to analyze web and mobile ecosystems. Published at top-tier venues (ACM CCS, IEEE S&P) and released open-source tools adopted by external research groups. Industry experience applying generative AI in enterprise settings.

Work Experience

Radboud University *2021 – Present*
PhD Candidate – AI for Digital Privacy Analysis The Netherlands

- Led multiple research projects from problem definition to open-source release
- Designed and evaluated GenAI solutions including autonomous app navigation with multimodal LLMs, prompt-injection guardrails, and large-scale web measurement systems
- Supervised master and bachelor students

VaultJS *Jan 2026 – Present*
Privacy & AI Consultant United States (Remote, part-time)

- Building an LLM-based navigation agent to explore mobile apps and monitor data flows for privacy compliance
- Advising on prompt-injection risks and mitigation strategies for AI-driven app analysis pipelines

ING *Apr 2025 – Sep 2025*
Generative AI Engineer – Internship The Netherlands

- Designed and developed a multi-agent LLM pipeline for legacy code migration (2.5M lines PL/SQL to Java), including prompt optimization, retrieval-augmented API grounding, and compiler-feedback evaluation loops
- Collaborated with software engineers and architects to understand requirements and present results and recommendations to technical and business stakeholders

University of Twente *Oct 2023 – Dec 2023*
Visiting Researcher The Netherlands

- Designed the initial LLM-based iOS automation approach during a research visit, which evolved into an open-source library

MarWell Bio *Sep 2020 – Sep 2021*
Machine Learning Researcher United States (Remote, part-time)

- Designed and developed deep generative models for therapeutic antibody discovery targeting SARS-CoV-2

Selected Projects

LegacyTranslate – Multi-Agent Code Translation *2025*

- Designed and implemented LLM-based agents for code translation, API grounding via retrieval, and compiler-feedback refinement for PL/SQL to Java migration; achieved 53.6% compilable output and 33.9% test-pass rate

AI Guardian – Browser Extension for LLM Guardrails *2025 – 2026*

- Developed a Chrome extension that intercepts built-in AI API calls by websites and detects prompt-injection attacks; measured AI API usage across top 50K websites

WhisperTest – LLM-Powered iOS UI Automation *2024 – 2025*

- Developed an open-source iOS automation library using multimodal LLMs and Apple's Voice Control to navigate apps without jailbreaking; enabled fully automated dynamic analysis of iOS apps at scale

Targeted & Troublesome – Web Privacy at Scale *2023 – 2024*

- Built a multilingual ML classifier over 2M+ web pages and a crawling pipeline across thousands of websites; revealed third-party trackers and improper ads on child-directed sites

Bitter Pill – Pharmacy Website Privacy Analysis *2025*

- Analyzed tracking on pharmacy websites across EU countries; uncovered new tracking methods such as server-side tracking, CNAME-based tracking, as well as re-targeted ads for sensitive health products

VAEResTL – Generative Model for Antibody Design *2020 – 2021*

- Built a deep generative model to generate CDR-H3 sequences for SARS-CoV-2 antibodies

Education

Radboud University *2021 – Present*
Ph.D. Candidate, Digital Security The Netherlands
- Topic: Applied machine learning for large-scale web and mobile privacy analysis

Shiraz University *2017 – 2020*
M.Sc. Computer Engineering, Secure Computing Iran
- Thesis: Malware Detection Using Generative Models Based on Deep Learning

University of Isfahan *2013 – 2017*
B.Sc. Software Engineering Iran

Technical Skills

Languages: Python, JavaScript, Java, SQL
ML Frameworks: PyTorch, TensorFlow, Keras
AI Techniques: LLMs, VLMs, RAG, GANs, Transformers, LLM-based agents, Prompt engineering, Guardrails
Libraries & Tools: Pandas, NumPy, NLTK, Matplotlib, Scikit-learn, Jupyter Notebooks, Playwright, Puppeteer
Infrastructure: Git, Linux, Docker, AWS, Azure

Selected Publications

Venues including ACM CCS (14% acc. rate) and IEEE S&P (15% acc. rate).
- **EASE 2026** – LegacyTranslate: LLM-based Multi-Agent Method for Legacy Code Translation *(under review)*
- **IWPE 2026** – Local Models, Global Risk: Assessing Emerging Threats in Local AI APIs in Browsers *(under review)*
- **ACM CCS 2025** – WhisperTest: A Voice-Control-Based Library for iOS UI Automation
- **DPM 2025** – The Bitter Pill: Tracking and Remarketing on EU Pharmacy Websites
- **IEEE S&P 2024** – Targeted and Troublesome: Tracking and Advertising on Children's Websites
- **Bioinformatics 2022** – VAEResTL: A Novel Generative Model for Designing CDR of Antibody for SARS-CoV-2
- **Ad Hoc Networks 2021** – Generative Adversarial Network to Detect Unseen IoT Malware

Certifications & Training

Retrieval Augmented Generation (RAG) – DeepLearning.AI & AWS, Coursera *2025*
Generative AI with Large Language Models – DeepLearning.AI & AWS, Coursera *2023*
Security and Privacy in the Age of AI – KU Leuven *2022*

Talks

Dutch Data Protection Authority (AP), Den Haag – Invited talk, iOS UI Automation using AI *2026*
CNIL Privacy Research Day, Paris – Invited panelist, Tracking & Advertising on Children's Websites *2024*
ETH Zurich, Information Security Group – Invited talk, Targeted and Troublesome *2024*
NWO ICT.OPEN, Utrecht – Online Tracking and Advertising *2023*

Academic Service

Program Committee Member:
- The ACM Web Conference 2026
- European Workshop on Systems Security (EuroSec) 2026
- Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2026
- USENIX Security (poster session) 2024

Languages

English (C1) · Persian (Native) · Dutch (A2)

References

Dr. Gunes Acar, Assistant Professor – Radboud University
g.acar@cs.ru.nl gunesacar.net
Dr. Andrea Continella, Associate Professor – University of Twente
acontinella@iseclab.org conand.me
Jonck van der Kogel, Chapter Lead – ING
Jonck.van.der.Kogel@ing.com RocketReach