





# HOSSEIN KHALILI

 [hosseinhkh.com](https://hosseinhkh.com)  [hkhalili@ucla.edu](mailto:hkhalili@ucla.edu)  [linkedin.com/in/hossein-khalili](https://linkedin.com/in/hossein-khalili)  [Google Scholar](#)

## Summary

Amazon Fellow and Ph.D. candidate in Electrical and Computer Engineering at UCLA specializing in large language models (LLMs), diffusion models, and adversarially robust, privacy-preserving machine learning. Former CTO at Digify (part of Digikala), where I led the development of AI-driven products at scale. With over a decade of experience in software engineering, machine learning, and IoT systems, I bring a multidisciplinary background that also spans electrical engineering and cybersecurity. My expertise lies in building high-performance and robust AI and IoT solutions, with a particular focus on large language models (LLMs) by improving their performance, enhancing privacy, and strengthening security to translate cutting-edge research into real-world applications.

## Education

### University of California, Los Angeles (UCLA)

Los Angeles, CA

*Ph.D. in Electrical and Computer Engineering; GPA: 4.0*

*Sep. 2023 – 2027(Expected)*

– **Advisor:** Prof. Nader Sehatbakhsh

– **Research Focus:** Security and Privacy in Machine Learning, Large Language Models (LLMs), Computer Vision

### Sharif University of Technology

Tehran, Iran

*M.Sc. in Computer Science (Artificial Intelligence and Robotics); GPA: 19.63/20*

*Sep. 2020 – May 2023*

– **Thesis:** 3D Medical Image Segmentation using Unlabeled Data

### Sharif University of Technology

Tehran, Iran

*B.Sc. in Electrical Engineering and Physics (Double Major); GPA: 16.85/20*

*Sep. 2013 – Sep. 2019*

## Selected Publications

### LightPure: Realtime Adversarial Image Purification on Mobile Devices

MobiCom 2024

*H. Khalili, S. Park, V. Li, B. Bright, A. Payani, R.R. Kompella, N. Sehatbakhsh*

### Detecting Keystrokes in VR via External Side-Channels

IEEE S&P Workshops 2024

*H. Khalili, A. Chen, T. Papaïakovou, T. Jacques, H.-J. Chien, C. Liu, A. Ding, N. Sehatbakhsh*

### Context-Aware Hybrid Encoding for Privacy in IoT Devices

IEEE 2023

*H. Khalili, H.-J. Chien, A. Hass, N. Sehatbakhsh*

### Enc2: Privacy-Preserving Inference for Tiny IoTs via Encoding and Encryption

MobiCom 2023

*H.-J. Chien, H. Khalili, A. Hass, N. Sehatbakhsh*

## Professional Experience

### Digify (Part of Digikala Group)

Tehran, Iran

*Co-Founder and Chief Technology Officer*

*Aug. 2021 – Aug. 2023*

- Digikala is the largest e-commerce platform in Iran, comparable to Amazon.
- Architected and developed Digify.shop, an e-commerce platform offering shop builders and headless commerce solutions.
- Led technical design and implementation of scalable systems, enhancing platform reliability and performance.
- Led hands-on development using technologies such as Python, Django, React.js, and Kubernetes.

### Bonus

Tehran, Iran

*Co-Founder and Chief Technology Officer*

*May 2016 – July 2021*

- Co-founded Bonus, developing advanced loyalty platforms and AI-driven customer engagement tools.
- Designed and implemented over ten successful products, focusing on backend and frontend development.
- Worked with Python, PHP, Laravel, MySQL, JavaScript to develop high-performance APIs and integrate machine learning models for enhanced user experience.

### Carriot

Tehran, Iran

*Founder and Technical Lead*

*June 2017 – Feb. 2019*

- Developed IoT-based car tracking devices and platforms for real-time vehicle monitoring.
- Programmed firmware for embedded systems using C++ and Assembly, optimizing real-time performance and implementing efficient communication protocols like MQTT and Protobuf.
- Built mobile applications for device control and data visualization.

## Technical Skills

---

**Programming Languages:** *Advanced:* Python, C++, Java, JavaScript, PHP    *Proficient:* Go, Kotlin, R, MATLAB

**Machine Learning & AI:** PyTorch, TensorFlow, Keras, scikit-learn, ONNX, XGBoost, QAT, Transfer Learning, RL, Knowledge Distillation, Reward Modeling

**Generative Models & LLMs:** GPT, Llama, Stable Diffusion, Prompt Engineering, Multi-turn Prompting, Diffusion-Based Defenses, Fine-tuning with LoRA / QLoRA, RLHF (Reinforcement Learning from Human Feedback)

**Cloud, DevOps & MLOps:** Docker, Kubernetes, AWS, GCP, Azure DevOps, Terraform, CI/CD (GitHub Actions, Jenkins, GitLab CI/CD), DeepSpeed, MLflow, KubeFlow

**Data Engineering & Pipelines:** Kafka, REST, GraphQL, Protobuf, MQTT, Elasticsearch, ML Pipelines

**Web & Front-end:** Django, Flask, Laravel, React.js, Vue.js, Nuxt.js, Node.js, Redux, Sass, Apollo GraphQL

**Databases:** PostgreSQL, MySQL, MongoDB, Redis, SQLite

**Expertise Areas:** Adversarial Robustness, Privacy-Preserving ML, LLM Security, Computer Vision, Audio Classification, IoT Development, High-Performance Computing, Differential Privacy

**Additional Tools & Methodologies:** Git, GitLab, Bitbucket, TDD/BDD (PyTest, JUnit, RSpec), Agile/Scrum, JIRA, Confluence, Prometheus, Grafana, ONNX Runtime, TensorRT

## Research Experience

---

### Graduate Researcher

*Sep. 2023 – Present*

**UCLA**  
*Los Angeles, CA*

- **LLM Jailbreaking & Defense:**
  - \* Investigated multi-turn jailbreak prompts to expose vulnerabilities in LLMs.
  - \* Proposed fine-tuning strategies to mitigate harmful text generation.
- **Privacy-Preserving LLM Interface:**
  - \* Developed a local LLM-based pipeline to mask private tokens before cloud-based inference.
  - \* Ensured robust data protection with minimal impact on accuracy.
- **LightPure & Adversarial Robustness:**
  - \* Created a real-time adversarial image purification method using diffusion models on mobile devices (up to 10x speedup).
  - \* Combined adversarial training with real-time diffusion for higher accuracy under attack.
  - \* *Accepted at MobiCom 2024.*
- **Multi-Camera Semantic Segmentation for VR:**
  - \* Developed a privacy-preserving pipeline to mask sensitive objects across multiple VR camera feeds in real time.
  - \* Employed superpixel-based segmentation for efficient multi-view object detection and concealment.
- **SuperPure:**
  - \* Innovated a defense strategy combining downsampling with diffusion-based super-resolution to thwart adversarial patches.
- **LLM for Robotics:**
  - \* Exploring GPT-based frameworks for high-level robot control and instruction parsing.

### Graduate Researcher

*Sep. 2020 – May 2023*

**Sharif University of Technology**  
*Tehran, Iran*

- **Audio-Based TB Detection:**
  - \* Co-led a project detecting TB from cough audio using deep neural networks.
  - \* Applied transfer learning from large-scale speech models for limited-data scenarios.
- **3D Medical Image Segmentation:**
  - \* Enhanced 3D U-Net with ConvLSTM to capture spatio-temporal features in volumetric data.
  - \* Achieved higher Dice coefficients on organ segmentation with minimal parameters.
- **VoxelMorph Augmentations:**
  - \* Improved unsupervised registration accuracy using superpixel-based augmentations for CT/MRI scans.
  - \* Reduced alignment errors and enhanced diagnostic reliability.
- **Hybrid Model (Weakly Supervised Segmentation):**
  - \* Combined 3D U-Net and VoxelMorph with superpixel post-processing, boosting performance in limited-label settings.
- **Persian Poem Generation:**
  - \* Built an NLP pipeline generating Persian poems from a large corpus of classic/modern text.
  - \* Focused on rhyme, meter consistency, and thematic coherence.

## Selected Projects

---

### LLM-based Teaching Assistant for Children

2024

- Conceptualized and developed a **child-friendly AI tutor** that generates interactive learning materials, story-driven content, and age-appropriate skill-based exercises.
- Integrated **adaptive difficulty** based on student performance, progressively tailoring lessons to maintain engagement and learning efficacy.
- Built a **web-based interface** with real-time feedback, analytics, and parental controls, fostering a safe and supportive environment.

### Instagram Product Search Engine

2021

- Built an **NLP-driven** system to index and analyze **Instagram posts/comments** for product listings, prices, and brand mentions.
- Leveraged **Elasticsearch** for efficient text indexing and real-time searching across high-volume data.
- Developed **custom text-mining heuristics**, including contextual keyword extraction and price detection, for robust data parsing.
- Implemented a **scalable data ingestion** pipeline with Python & REST APIs, enabling continuous updates from active Instagram feeds.
- Engineered sorting algorithms (e.g., price-based, popularity-based) to deliver **sub-second query responses** and enhance user experience.

### Point-of-Sale (POS) System

2019 – 2020

- Architected and developed a full-stack POS solution using **Python (Django)**, **React.js**, **PostgreSQL**, and **Socket.IO**, supporting real-time analytics and seamless user experience.
- Implemented **microservice architecture** with Docker, enabling flexible deployment, scaling, and maintainability.
- Integrated dynamic **inventory management**, **live sales tracking**, and secure **role-based authentication** for shop owners and employees.
- Developed **interactive dashboards** to monitor sales performance, track inventory, and visualize customer insights.
- Ensured multi-platform support (web and mobile) with **RESTful APIs** for integration with external services (e.g., payment gateways).
- Optimized queries for high-traffic scenarios, maintaining **sub-second response times** under peak loads.

### SSR E-commerce Application

2019

- Created a **server-side rendered (SSR)** platform (PHP/Laravel, Vue.js, Nuxt.js) to provide a dynamic storefront.
- Employed caching, load balancing, and pre-rendering to handle high traffic with minimal page load times.
- Incorporated advanced product categorization and recommendation modules, boosting user conversion rates.

### IoT Car Tracking Device

2018

- Developed embedded firmware in **C++/Assembly** using MQTT & Protobuf for low-latency data transfer and remote diagnostics.
- Built an Android application with live vehicle telemetry, geo-fencing, and predictive maintenance alerts.
- Implemented **battery optimization** strategies and robust crash/failure handling to ensure continuous data logging in varied environments.

### Anti-Cheating Step Counter

2016

- Engineered an ML-based step counter for a **paid-to-walk** platform, preceding modern wearable devices.
- Combined sensor fusion (accelerometer, gyroscope) with anomaly detection to accurately flag fraudulent.
- Enhanced user retention by integrating gamification elements, leaderboards, and daily walking goals.

### Insurance Portal Web App

2017

- Developed a **full-stack application** (Laravel, MySQL, Vue.js) for managing insurance quotes, user policies, and administrative tasks.
- Integrated dynamic reports for claim tracking, policy renewals, and user analytics.
- Implemented secure authentication and role-based authorization, ensuring compliance with insurance data regulations.

### Admin Dashboard (Single-Page App)

2017

- Developed a **Vue.js** SPA with Sass and Axios for real-time data CRUD, system monitoring, and user management.
- Employed **role-based access control** and modular UI components, enabling rapid feature additions and consistent user flows.
- Incorporated asynchronous updates and WebSockets for live notifications and event monitoring.

### SMS Manager with Lossless Compression

2016

- Built an Android application applying **custom compression algorithms** to store SMS archives with minimal storage overhead.
- Designed an efficient indexing mechanism for near-instant searching and retrieval of historical messages.
- Ensured fail-safe data handling to preserve critical text content, even under device constraints.

Awards and Honors

Amazon Fellowship	Amazon AI PhD Fellowship Program
2025	Los Angeles, CA
Gold Medalist	International Olympiad of Astronomy and Astrophysics
2013	Volos, Greece
Gold Medalist	Iranian National Astronomy and Astrophysics Olympiad
2012	Tehran, Iran

Leadership & Volunteering

Co-Chair of Executive Team of ISC (Iranian Students of California)	Los Angeles, CA
California	2025 – Present
– Responsible for overseeing strategic direction, partnerships, and event planning across multiple campuses in California.	
– Foster collaborations with local industry, cultural organizations, and academic institutions.	
Treasurer, ECE Graduate and Professional Association (ECEGAPS)	Los Angeles, CA
University of California, Los Angeles	2024 – Present
– Manage financial records, budgeting, and resource allocation to support ECEGAPS initiatives.	
– Organize events and workshops in collaboration with the ECE department to promote professional development.	
– Coordinate with faculty, staff, and external sponsors to secure funding and enhance departmental engagement.	
Director of IGPA (Iranian Graduate and Professional Association)	Los Angeles, CA
University of California, Los Angeles	2023 – 2025
– Organized and led events supporting Iranian graduate students, including academic workshops and networking sessions.	
– Advocated for student resources and funding through direct collaboration with university administration.	

Teaching & Mentorship

Mentor	UCLA - Ssysarch Lab
2023 – Present	Los Angeles, CA
– Mentored and led 12+ undergraduate researchers on cutting-edge research in LLM security, adversarial robustness, and diffusion-based defenses, guiding them in experimental design and implementation.	
– Supervised projects on LLM jailbreak detection, adversarial purification using diffusion models, and secure generative AI, leading to the submission of three peer-reviewed papers.	
Teaching Assistant	UCLA
2025	Los Angeles, CA
– Served as TA for UCLA ECE 209AS.	
Teaching Assistant	Sharif University of Technology
2020 – 2023	Tehran, Iran
– Served as TA for graduate courses in Deep Learning, NLP, MRI, Medical Image Analysis.	
– Guided student projects on 3D image segmentation, advanced ML pipelines, and performance optimization.	
Astronomy & Physics Coach	Various High Schools
2012 – 2015	Iran
– Trained high school students for national Olympiads in Astronomy/Physics, covering theory and observational techniques.	

Relevant Coursework

• Machine Learning	• Diffusion Models	• Parallel Computing	• Adv Software Eng
• Deep Learning	• LLM	• GPU Programming	• Large-Scale Data Sys
• Adversarial ML	• NLP & Transformers	• RL	• Cloud & Edge Comp
• Security & Privacy in ML	• IoT Security	• HCI for AI	• Adv ML Architectures

Personal Profile

Key Strengths & Work Style
– Results-Driven Finisher: Consistently brings projects to completion, ensuring on-time delivery and high quality.
– Decisive Leader: Makes swift, well-informed decisions under pressure, balancing risks and opportunities to propel teams forward.
– High-Energy Influencer: Infuses the work environment with enthusiasm, motivating colleagues and boosting team morale.
– Adaptable Problem-Solver: Thrives in dynamic environments, quickly learning new technologies and approaches to overcome challenges.
– Team Builder & Mentor: Excels at fostering cross-functional collaboration, mentoring talent, and empowering individuals to reach their potential.
– Persistent & Resilient: Displays unwavering determination; leverages creativity and grit to accomplish ambitious goals without giving up.